(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80190 A1

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number: PCT/CA01/00504

(22) International Filing Date: 17 April 2001 (17.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,305,249 14 April 2000 (14.04.2000) CA

(71) Applicant *(for all designated States except US)*: **CYBERUN CANADA CORP.** [CA/CA]; 25 McArthur Street, Etobicoke, Ontario M9P 3M6 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SARCANIN, Branko** [CA/CA]; 25 McArthur Street, Etobicoke, Ontario M9P 3M6 (CA).

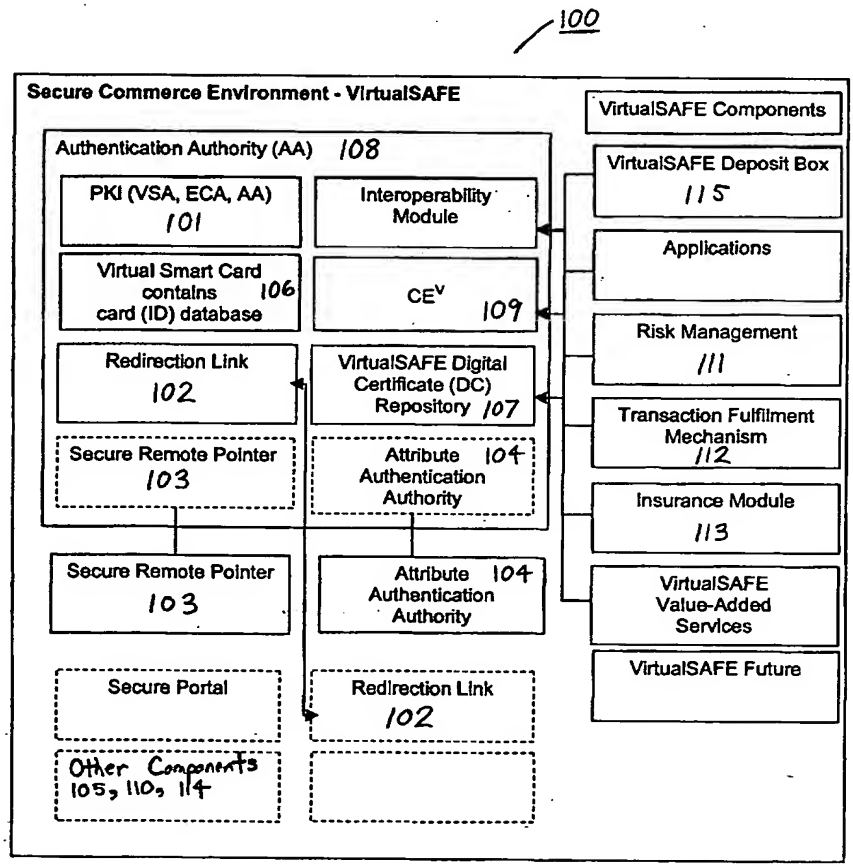
(74) Agents: **PILLAY, Kevin** et al.; Fasken Martineau DuMoulin LLP, Toronto Dominion Bank Tower, Box 20, Suite 4200, Toronto-Dominion Centre, Toronto, Ontario M5K 1N6 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: A METHOD AND SYSTEM FOR A VIRTUAL SAFE



(57) Abstract: A transaction server for performing a transaction over a network using a virtual smart card the server comprising, a virtual smart card database having a plurality of records each record including a virtual card identification and a value corresponding to a single virtual smart card; a security module; an emulator for emulating a smart card, the emulator for receiving smart card commands and processing the commands in conjunction with the virtual smart card database and the security module; and a virtual card reader module for receiving the smart card commands and relaying the commands to the smart card emulator whereby transactions are performed over the network using one or more the records and the virtual smart card database.

WO 01/80190 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD AND SYSTEM FOR A VIRTUAL SAFE

The invention relates to the field of electronic commerce. More specifically, the invention relates to electronic commerce with virtual smart cards and virtual safes.

BACKGROUND OF THE INVENTION

There has been a rapid increase in the number of consumers with access to the World Wide Web, there has been a great deal of interest in the development of electronic commerce on the Internet. However, anxieties concerning online security are presently undermining the evolution of electronic business as they attenuate the trust between companies and trading partners, as well as between online retailers and consumers. In traditional business transactions, trust is established face-to-face and supported by documentation that eliminates liability. Today, traditional financial transactions are being transformed. In particular, possibilities for the use of smart cards are expanding.

A smart card, also called a chip card, integrated circuit card, memory card or processor card, is typically a credit card-sized plastic card that includes one or more semiconductor integrated circuits. A smart card can interface with a point-of-sale terminal, an ATM, or with a card reader integrated with a computer, telephone, vending machine, or a variety of other devices. The smart card may be programmed with various types of functionality such as stored-value applications, credit or debit applications, loyalty applications, cardholder information, etc. Although a plastic card is currently the medium of choice for smart cards, it is possible to implement these cards using a smaller form factor. For example, a smart card could be attached to a

key chain or it could be as small as a single integrated circuit chip. A smart card may also be implemented as part of a personal digital assistant, telephone, or some other form.

Typically, a smart card contains a hardware encryption module for performing a variety of encryption algorithms. Encryption may also be performed in software. A typical environment for issuing smart cards and for reconciling transactions performed with such cards in the consumer context may be described as follows. A terminal supplier builds the equipment used by a service provider to provide goods and/or services to consumers via smart card and a service payment terminal. A card supplier contracts with an integrated circuit manufacturer and a card manufacturer for integrated circuits and plastic card bodies, respectively. The card supplier then embeds the integrated circuits in the cards and initializes them with a serial number. The card supplier then delivers these cards to a card issuer. In conjunction with a clearing and administration system, the card issuer personalizes new cards and then transfers these cards to individual cardholders (i.e. consumers). A cardholder may then charge the card with value prior to use. Alternatively, the card may be delivered with value pre-loaded. The cardholder may then use the card at a service payment terminal to purchase goods and/or services from the service provider. Upon purchase, the terminal debits the value of the purchase from the card, thus creating a service payment. The system may be implemented, for example, using Visa, MasterCard, American Express, Discovery, Players Card International, bank and financial institution debit cards, and other cards.

In this typical environment, all transactions are sent in a data file from the service payment terminal, via an acquirer, to a clearing and administration system. Accumulated service payment batches from other terminals are also sent to the clearing and administration system. Based upon this collection data, the clearing and administration system receives money from the card issuer. The money received from the card issuer, of course, originates from the cardholder. The clearing and administration system then transfers a lump sum to the acquirer using a suitable settlement service (e.g. Visa, MasterCard American Express, Discovery, Players Card International, etc.) to pay the various service providers having a relationship with the acquirer. Based upon the collection data, the acquirer then transfers an appropriate amount of money to each service provider reflecting the value of the goods and services that that service provider provided to cardholders that day. The value of the goods and services provided is based, of course, upon deductions from cardholders' smart cards.

A consumer typically uses a service payment terminal in a face-to-face environment in order to purchase goods in a store or directly from the terminal itself. The service payment terminal can be an attended device or it can be integrated into a self-service device such as a vending machine or public telephone. For example, the service payment terminal may be incorporated into a soda machine in order to dispense sodas to a customer where the customer pays by inserting the smart card. Or, the service payment terminal may be a point-of-sale terminal (i.e. POS) typically found at a check-out counter wherein a consumer inserts his smart card in order to purchase goods.

In general, service payment terminals allow consumers to use smart cards for the payment of goods and services. A service payment terminal generates a payment result from a transaction and bundles individual payment results into a collection for transfer to a clearing and administration system. The service payment terminal then transfers funds debited from consumers' smart card to the merchant whose goods and services were purchased through the terminal. Thus, a variety of goods and services may be purchased using a smart card from a merchant having a service payment terminal on premises. In addition, a consumer with a smart card may purchase goods or services from a merchant over the Internet.

Now, in order to purchase a product or service, the card must first be loaded with value. Value can be loaded onto a "stored-value" card in a variety of ways. For example, it is often inconvenient for a consumer to load value onto his or her smart card. The consumer must physically travel to a bank or other institution that has an automated teller machine (ATM), or other similar device, in order to load value onto the smart card. With respect to loading value onto a smart card, the consumer may insert money into a value loading machine and have a corresponding value put onto the smart card. Or, the consumer may use a debit card to deduct value from the consumer's bank account for transfer to the card. Additionally, a credit card can be used as the source of funds to be transferred to the smart card. In these circumstances, the consumer must travel to the bank to load value. A further inconvenience exists in that not all banks or other financial institutions have such machines for loading value onto smart cards. A technique by which consumers may conveniently load value onto their smart cards via the Internet is described in U.S. Patent Application No. 09/070,488 (Davis, et al.), filed April 30, 1998, and entitled "Internet Loading System

Using Smart Card", which is incorporated herein by reference. However, it is desirable in some situations to be able to use such payment and loading systems without having a physical smart card.

One problem with the systems described above is that they are dependent on the deployment of two hardware components new to the mass consumer market: smart cards and smart card readers (either stand alone or integrated with some form of personal electronic device such as a mobile telephone or computer keyboard). Smart cards and smart card readers represent relatively new technology that raise corresponding issues of reliability, cost, market acceptance, and distribution. Although the above-described systems could technically be implemented, the lack of a large number of smart cards and card readers in public use raises infrastructure related difficulties.

However, the above-described systems do present many benefits for electronic commerce. As cash may not be an option in many situations, the above systems offer a compelling solution for merchants selling products and services on-line in situations where, physically, those products and service have low monetary value. The deployment of such systems, however, is again hampered by a lack of smart cards and smart card readers. This problem is exacerbated in that the card reader market is not well developed from a standards perspective which in turn raises potentially significant interoperability issues. Simply put, a practical problem exists in that without having large numbers of smart cards and card readers in use, there is little demand for them from consumers, which in turn makes it difficult to convince merchants to adopt such systems.

Therefore, a need exists for a method and system that may quickly and easily allow consumers and merchants to use the above-described systems without requiring that physical smart cards and smart card readers be distributed and installed first. Such a method and system should provide a fast and inexpensive alternative for users of the above-described systems to take advantage of the opportunities of the electronic marketplace. Such a method and system would allow merchants and issuers to establish a market presence that would in turn eventually facilitate the acceptance of physical smart cards and card readers when those hardware components become more readily available.

Now in traditional business transactions, trust is established face-to-face and supported by documentation that eliminates liability. In the electronic world, where companies of all sizes are increasingly conducting commerce between virtual trading communities, trust must be established in seconds between strangers who are physically separated. At the heart of this trust issue is the concept of authentication, or the burden of proving the identity of the parties involved in a transaction. Information can be deemed secure only when it is provided or accessed by authorized parties, exclusively. Consequently, effective security is based on the unequivocal authentication of authorized parties. A need therefor exists for an improved level of security in online authentication. Such improved security will help eliminate the current constraints on businesses, governments and individuals to fully leverage the flexibility and advantages of communicating and transacting over the Internet and also over intranets, extranets, and enterprise networks.

For reference, an overview of existing digital signature technology, the public key infrastructure (PKI), and electronic commerce payment policy X9.59 is presented in the following.

Traditional Digital Signature Methodology. For commerce to occur on the Internet, contracts must exist. For contracts to exist, signatures are required. It is becoming increasingly accepted that digital signatures will suffice as binding signatures for Internet commerce. Therefore, digital signature will be a core component in the realization of true electronic commerce.

Digital signatures rely on the public key infrastructure ("PKI"). The PKI model involves an entity, such as a consumer, having a pair of encryption keys: one private, one public. These keys work in concert to encrypt, decrypt, and authenticate messages. One method of authentication is through the application of a digital signature. Consider the following example:

- The buyer (i.e. a client software program on the buyer's PC) creates a message (e.g. purchase order) that he or she wishes to digitally sign.

- The buyer runs the message through a hashing algorithm to produce a hash or digest of the message. The digest is unique for every message. It is essentially a digital fingerprint of the message in a much smaller form which makes it more economical to encrypt than the message itself.

- The digest is encrypted with the buyer's private key to form the digital signature. A digital signature is a message digest encrypted with a private key.

- The buyer then sends the following to the merchant: the message (e.g. purchase order and account number); the digital signature; and, the buyer's public key.

- To validate the signature, the merchant performs the following steps: the merchant (i.e. transaction server) runs the message through the standard hashing algorithm (i.e. the same one used by the buyer) to produce a digest of the message received; the merchant uses the buyer's public key to decrypt the digital signature (i.e. the digital signature was produced using the buyer's private key to encrypt the message digest, therefore, when decrypted with the buyer's public key it produces the same digest); the merchant compares the first digest with the second digest produced, if the digests match exactly, then the merchant has confirmed the following:

  - The message was not tampered with in transit. Changing a single bit in the message sent from the buyer to the merchant would cause the second digest to be different than the first digest. If they are different, then the transaction fails.

  - The public key used to decrypt the digital signature corresponds to the private key used to create it. No other public key could possibly work to decrypt the digital signature, hence, the merchant was not given someone else's public key.

  - If the first digest matches the second digest exactly, then the merchant has confirmed the above but has not yet confirmed

that the public key used to decrypt the message is valid or that the public key is owned by the buyer (i.e. whose credit card account, bank account, etc., is going to be debited).

In the above scenario, the buyer could very well use his or her own private key to digitally sign a payment authorization on the buyer's account. A digital signature applied with the buyer's private key and validated with the buyer's public key will work perfectly well. The merchant has no way of knowing that it does not correspond to the buyer's bank account. Due to this potential of uncertainty about key pairs, the merchant needs a method of ensuring that the public key is trustworthy. Currently, the typical solution to this problem is to rely on digital certificates issued by a third-party Certification Authority ("CA").

Now, a digital certificate is not a digital signature. Signatures are unique for each message (i.e. the unique digest of the message encrypted with the sender's private key). On the other hand, a digital certificate is the user's public key to which the CA has applied a digital signature. Functionally, it is the CA's method of guaranteeing public keys. In addition, the certificate usually identifies the user in some way. In financial applications, one way of identifying the user is to bind the public key to the user's account. For example, this is the method used in Secure Electronic Transactions ("SET") which is a specification for processing credit card transactions over the Internet.

One of the problems with the use of digital certificates is that they themselves often have to be validated. For example, a Certification Authority may apply expiration dates to certificates or a CA may revoke certificates because of fraudulent use. As

such, more complex signature validation systems are required. There has to be some way of knowing that the digital certificate, which was issued at some point in the past, is still valid. The typical solution to this problem is the certificate revocation list ("CRL"). CRLs are meant to be accessed online, optionally (although preferably) in real-time, to guarantee that the certificate itself had not expired or been revoked since being issued to the user.

Now, certificate-based commerce relies on trust in the Certification Authority. Since not all Certification Authorities are known or necessarily trusted by parties to a transaction, these types of transactions often require certification of the Certification Authorities themselves. In general, there has to be a common denominator of trust between the two parties to a transaction for that transaction to take place. This need typically results in the use of multiple certificates, one layered on top of another, in a single transaction. Each CA is essentially guaranteeing the integrity of its sub-CAs. This is what is known as a CA hierarchy. Therefore, in order to obtain a user's public key to validate a digital signature, the receiver in the transaction may have to peal off multiple digital certificates, each through a relatively intensive cryptographic operation. As such, transaction times can be dreadfully slow.

The traditional digital signature model is a complex and computationally expensive process for issuing, applying and validating digital signatures and is not likely to succeed for mainstream financial transaction processing over the Internet. The problems with the traditional digital signature arise because it was not developed specifically for today's financial transactions. A need therefore exists for a secure means to conduct electronic commerce that takes into account the infrastructure and

business processes already in place within the financial sector to ensure trust in financial transactions.

Public Key Infrastructure (PKI). Public key digital signature technology may represent part of a strong authentication business process. However, it only represents part of a business process infrastructure. What is also required is a means for binding the digital signature to something that has meaning within the business process. Currently, there is much interest in public keys and the use of digital certificates for new electronic commerce applications. Digital certificates provide a mechanism for binding a public key to an identity or set of attributes where there is no existing binding infrastructure.

The traditional PKI infrastructure involves the issuing of certificates that are signed by a Certification Authority which demonstrates the validity of the public key, checks the validity of the private key, and provides some identity information for the entity that is issued the certificate. The associated PKI model involves an entity "digitally signing" a document with their private key and then "pushing" the transaction document, the digital signature, or a copy of the digital certificate to another party. The receiving party validates the authenticity of the digital-signature and the originator's public key via the contents of the associated digital certificate (as well as processing the certificate supplied identity and/or attribute information). Originally, the contents of the digital certificate were assumed to be sufficient such that digital signature validation and identity/attribute processing could be performed without any additional electronic transmissions. However, as the technology matured, it became apparent that more and more complex verification mechanisms were

needed. For example, a check for changes in status between the time that the certificate was originally manufactured and the present is required, as a minimum. As discussed above, certificate revocation lists (CRLs) were developed in an attempt to partially address the issue of current real-time status in the offline verification model. In fact, many existing business infrastructures use account-based methodology as a means of binding attributes. For example, several account-based business processes support non-face-to-face transactions using authentication bindings such as "mother's maiden name", "social security number", and PINs.

Now, public keys may be added to existing non-face-to-face transaction capabilities (e.g. registering a public key for an account using processes similar for registering items such as an individual's mother's maiden name, social security numbers, and PINs). Such changes are minimal with respect to existing business processes (i.e. maintaining the current business process environment) while at the same time they allow for the extension of account-based business processes to strong authentication, electronic commerce transactions. In fact, there have been several electronic commerce pilot projects that have relied on certificate-based bindings in attempts to minimize software changes to existing business systems. However, for account-based business processes, the certificate-based bindings have not fit in well with standard business processes. To make electronic commerce a reality, it will be necessary to integrate public-key bindings into core account-based business processes. This will require changes to installed data processing systems. Without this integration, there is little hope of deploying electronic commerce on a large scale. The lack of business process integration, and the associated risks, outweigh any increased costs associated with modifying existing data processing systems. For example, an attempt to develop

a non-integrated certificate-based binding pilot project for an account-based business process will likely result, over the long term, in large increases in technology, software, and manpower due to the need for ongoing reconciliation of independent certificate-based bindings and account-based business processes bindings. Integration of public-keys into existing account-based business processes is the only reasonable method of scaling electronic commerce operations in those account-based operations.

A need therefore exists for a system that effectively incorporates the public key digital signature's strong authentication into existing business infrastructures hence enabling them for electronic commerce.

Electronic Commerce Payment (Policy X9.59). The main policy issue for an electronic commerce payment protocol, such as X9.59, is privacy. In a typical retail electronic commerce payment, a merchant is interested in knowing if funds will be paid. It is not necessary to know the identity of the consumer for this payment. It might be necessary to know an address for the shipment of goods, but not for payment. In response to this situation, policy X9.59 was developed. It assures a merchant of payment without having to divulge any consumer identity information. An X9.59 payment uses an account authority digital signature for the consumer's bank to authenticate the payment transaction.

Now, CA based digital signature transactions might typically carry with them X509v3 certificates. Such certificates normally include certain identity information (e.g. a person's "distinguished name" and address). In some CA based business scenarios, various fields in X509v3 identity certificates are truncated or redefined to minimize the amount of identity information and therefore the privacy exposure from using

them. In the account-based business world, the issue is primarily authentication, not identification. Any identity issues are part of the business process that establishes the account. Different account-based business processes have different identity requirements for establishing an account. If the business account-setup identity requirements are similar to identity requirements for a certificate, then such a certificate might be appropriate for an account establishment transaction. Normal account-based business transactions involve authentication and authorization against the information that is bound with the account. One issued that arises in the use of accounts for attribute binding is the requirement for real-time attributes, for example, the amount of money available in the account or the total charges outstanding to date.

Identity certificates in an account-based payment environment unnecessarily propagate individuals' private information. For example, providing extra information to a merchant when it is not necessary for the merchant to know more than that will be available to cover the transaction. Other types of attribute-based certificates are not necessary in an account-based environment because they duplicate the attribute binding function already provided by the account infrastructure. Furthermore, attribute certificates could actually create unnecessary fraud and risk problems where the certificate includes stale copies of attributes that are normally maintained in real-time at the account level.

Now, progression within the authentication field can be characterized as non-electronic and offline, electronic and online, and electronic and offline. The non-electronic and offline world is exemplified by drivers' licenses, letters of credit,

employee identification cards, etc. In the credit card world, printed invalid credit-card booklets are distributed to merchants on a regular basis.

Certificates were originally developed as electronic analogs of non-electronic methods. These original applications were offline but did involve technology such as point-to-point communications and stand-alone badge readers. This was also characteristic of the dominant mode of offline email systems wherein calls were made to an email server, queued email was exchanged, and then connections were broken. Actual email processing occured offline in machines that were only sporadically connected. Simple point-to-point exchange with a variety of different machines was typically involved.

Certificates may improve the identity and authentication processes in offline transactions where there is no access to any online account-based bindings. In such cases, certificates may represent an improvement in the level of confidence regarding the offline transaction. This is similar to the use of a driver's license to improve authentication in a retail check or credit transaction. In effect, the financial industry did not have the technical ability to authenticate consumers online and therefore reliance for this authentication was left to the merchant.

The transition to the electronic and online world may be epitomized by the current credit-card infrastructure. The credit-card industry has adopted an online paradigm involving real-time authorization which includes the checking of real-time credit-limit status.

In online business transactions, a certificate would typically represent a duplication of the binding information provided by a business account record. Use of the certificate could seriously degrade the transaction quality because the certificate binding might not be a one-to-one match with information required by the business process. Or, the certificate binding might represent stale information compared to that in the account record. Typically, certificate flows in an online account-based transaction would be unnecessary. However, such certificate flows may potentially degrade the quality of the transaction by:

- Unnecessarily divulging information such as identity to parties to the transaction.
- Creating a false impression of security where decisions are made based on certificate information that is stale or inconsistent with the business practice.
- Opening the infrastructure to unnecessary systemic risks such as attacks on the Certification Authority signing key and/or adding a requirement to contact an external Certification Authority.

In fact, a financial infrastructure with triple-redundant bunkered data centers in different geographically locations will not have its availability or integrity improved if dependencies to complete a transaction are introduced involving external sources.

The financial industry's X9.59 policy, is a light-weight, high integrity, strong authentication payment protocol targeted for all methods of electronic payment including, but not limited to, set-top boxes, point-of-sale terminals with online authorization, and merchant web servers. With the appropriate smart card, X9.59 can

work at point-of-sale, even improving the integrity of the current POS infrastructure, while eliminating the necessity for any identity information in payment transactions. A high-integrity smart card would eliminate additional authentication processes involving crosschecking of the name on the credit card with, for example, a driver's license. With the appropriate smart card, the account number and the digital signature for the transaction would be sufficient to satisfy high integrity requirements. In fact, a combination of the appropriate smart card, digital signature, and online network should provide the financial industry with the necessary components to authenticate consumers at retail locations.

A need therefore exists for a complete electronic payment and fulfillment system that may be conducted over a communications network.

In particular, approximately $350US billion in online purchase transactions occur between individuals and institutions each year. However, even greater use of the Internet for financial transactions has been limited by risks due to fraud, misrepresentation, or incomplete fulfillment. Individual Internet transactions are burdened by the need to have the transaction occur securely, quickly, and in a way that ensures that all parties are in receipt of goods or services and payment. Security must be achieved in an environment where the handling and managing of credit/debit and other financial transaction accounts is presently inconvenient for merchants and where delivery/fulfillment is costly and time consuming for both merchants and financial institutions. Although online transactions may be carried out under specific secure circumstances, such as the use of the Secure Sockets Layer ("SSL"), this method is very limited in its lack of purchaser authentication and fulfillment process

control. The existing Internet transaction methods de-couple payment and fulfillment and hence rely on multi-system solutions which are not necessarily secure.

For reference, today, financial transactions may take many forms including cash, check, credit card, debit card, automated teller, etc. Typically, the nature of the transaction determines which payment system is selected as follows:

- Financial payments ($500k+):

  Transactions in this range are predominantly payments between financial institutions using electronic systems such as CHIPS, FedWire and SWIFT.

- Commercial payments ($1000 to $500K):

  These are usually procurement payments between businesses. Since these transactions often require the exchange, EDI is commonly used.

- Consumer payments ($20 to $1000):

  At the higher end of the range, credit cards are generally used. While checks are also used, they have significantly less widespread acceptance, particularly among merchants, and are more often used for bill payment. At the lower end of this range, consumers are most likely to use cash. Credit cards are sometimes used as a cash substitute.

- Coin transactions (under $1):

Although the value of each transaction is low, the volume of transactions is high. These transactions are also highly diverse, ranging from buying newspapers to feeding parking meters.

Financial and commercial payments are already handled somewhat adequately by the systems which presently serve them. While improvements are possible, change is likely to be gradual. Transactions in the lower range are far less efficient. Consumer payments by credit card are appropriate where an extension of credit is required. However, because a credit card transaction is bundled with numerous supporting services, it is often ineffective as a substitute for cash, particularly for small value transactions. Cash transactions themselves are highly inefficient. In the year 2000, for example, Americans executed $300US billion in cash transactions for items costing less than $20. Banks and businesses spend over $60US billion annually to move, secure, and account for these transactions. In addition, growing numbers of consumers feel burdened by the inconvenience and risk of carrying cash. Furthermore, it is currently impossible to use cash in the electronic marketplace.

As such, low value cash and consumer transactions will likely be the heart of electronic commerce and electronic payment systems currently under development targeting this market. While not all cash transactions will migrate to electronic transfer, the development of a global network such as the Internet will itself create many new online markets. In this environment, a merchant will be any vendor who has Internet connectivity and offers goods and services for sale, whether they are durable goods, or information-based products such as reports and software entertainment. And, a consumer will be anyone who subscribes to the Internet and

browses vendor web sites for information or goods and services. This environment will give rise to a new type of payment transaction which has been referred to as a "micro payment." These payments will be of very low value, fractions of a penny in some cases, but executed in very high volumes. Micro payments will be used to purchase many of the new information based services that merchants or "information utilities" will offer to consumers. These information utilities must be able to bill in precise increments for their services including, for example, information retrieval (i.e. searching), cataloging, archiving, formatting, and reproducing in various media.

As discussed above, the many challenges faced by any electronic payment system include security which is the paramount requirement. However, in addition to being secure, the successful electronic payment system must protect individual privacy without impeding legitimate inquiries by law enforcement and government agencies. This requires transactional anonymity with an audit trail. In addition, allowance must be made for non-repudiated transactions which emulate cash transactions.

Now, for reference, electronic payment systems are typically based on either a credit card or a debit payment model. In the debit model, first an account is funded. Then, purchases are made using a debit card that credits the account. In the credit model, the purchase is made in advance of payment with a conventional credit card. Furthermore, electronic payment systems may be either online or offline systems. An online system is one where the parties to a transaction are joined through a network to a third party and communicate with this third party (i.e. server) during the course of the transaction. When transactions are executed on an online system, the server immediately records the transaction and updates various databases. It may also

initiate fund movements. On the other hand, in an offline system, two parties exchange funds without any communication with a bank or other third party during the transaction. Offline systems normally require hardware devices such as smart cards to provide adequate security. In order to download value (e.g. cash) onto the card, or to make a deposit, the card must be connected in some way to an electronic network to communicate with a bank or automated teller service. Until the device that receives a payment communicates with a bank over the network, the transaction is not documented within the banking system.

Existing payment systems can be categorized into the following types: debit systems, credit card based systems, electronic check systems, electronic coin systems, stored-value card systems, and electronic script systems. These systems, including their benefits and disadvantages, are briefly summarized in the following.

Debit Systems. Debit systems rely on the existing infrastructure of highly efficient automated clearinghouses ("ACH") and ATMs for initial funding. Therefore, they have relatively lower transaction costs as compared to credit systems. Typically, an ATM transaction costs $0.50US, or less, and an ACH transaction costs less than $0.15US. Only a single transaction is needed to fund an account. Debit systems execute payment transactions by exchanging electronic tokens. These tokens are digitally signed by a participating bank and delivered to the consumer in exchange for a debit to the consumer's checking account. The debited funds are held in an escrow account, so that the amount of digital cash or tokens issued is backed by an equivalent amount of cash. Today, debit systems normally use stronger security and authentication techniques than credit systems. Debit systems may employ public key

cryptography schemes for security and a variety of digital signature algorithms for authentication. This level of security allows debit systems to operate freely over open unsecured networks. Debit systems are an attractive alternative to cash for several reasons: transactions occur faster because there is no need to wait for change; debit systems eliminate the operational costs of handling cash; and, they improve security and reduce losses because businesses are able to transmit value to their bank at any time instead of having to wait for business hours to deposit cash. In addition, a key feature of the debit system is anonymity. However, only the payer receives complete anonymity. The payee can always be traced. It is believed that governments and law enforcement agencies will not accept security schemes that do not make provision for a so-called "back door". Moreover, it is not clear whether or not customers prefer complete anonymity in place of personalized contact with a merchant and protection against loss. The latter is only possible if records of tokens issued to consumers are kept on file. Common to all offline debit systems is the use of proprietary, special purpose hardware, including smart cards and the accompanying readers, wallets, and smart phones. Smart cards offer an added degree of freedom in dispensing with cash. A one-on-one transaction can be completed without a computer link provided the necessary hardware is available.

Credit card based systems. Presently, there are several electronic payment systems which are essentially existing credit card systems adapted for operation over the Internet. The main technical challenge they face in porting the functionality of the credit card system to the Internet is to securely obtain or transmit customers' credit card information. As a way to lower overall transaction costs, some credit card systems accumulate customer charges and merchant payments up to a predetermined

threshold before sending them out to processing agents. All electronic payment systems based on the credit card model benefit from the familiarity and name recognition these franchisees have carefully built up over many years of operation. However, given the average charge of about $0.20US, plus 2% to 3% transaction fees, most merchants would likely prefer to do business using an alternate, and less expensive, payment transaction scheme. Credit electronic payment systems are built around the conventional, bundled service credit card transaction processing systems. In the current environment, the only network transaction for which these electronic payment systems are optimized is a complicated cumulative charge and payment scheme. These systems are too costly and inefficient for the vast proliferation of low value payments, including micro payments, that will be common to electronic commerce in the near future. The privacy scheme for credit electronic payment systems, in most cases, is much like conventional credit card systems. Except for withholding credit card numbers, merchants have access to the standard customer information. Some of the systems provide authentication using digital signatures.

Electronic Check Systems. These are electronic payment systems that are equivalent to paper checks. An electronic check would typically consist of a document which is signed by the payer using a certified digital signature key. This key includes the information typically necessary for processing a paper check. This information may include the payer, the bank of the payer, the account number of the payer, the payee, the amount of the payment, and the date of the payment. The payee verifies the signature on the electronic check and then sends the electronic check to his bank for processing. The advantage of electronic checks is that they take advantage of existing bank clearing processes, which reduces development time. In a typical electronic

check model, the payee assumes the risk if the electronic check is no good. However, the merchant or payee would have two possible avenues to reduce their risk in the case of an online payment. If the bank was online, the payee could obtain approval from the bank that the check is good or could require that the payer obtain a certified check from a bank. The downside of electronic checks is their relatively high cost. Although they are expected to be considerably cheaper than credit card based systems, most developers of electronic check systems expect the cost to be in the $0.10US to $0.50US range per electronic check. Part of this cost is due to the necessity of an ACH (i.e. automated clearinghouse) transaction for each inter-bank check, which costs about $0.15US. Another problem with electronic checks is that they do not provide any privacy for the payer. The payee will know identifying information which is tied to the payer.

Electronic Coin Systems. There are numerous proposals for electronic payment systems that use electronic coins of fixed amounts as a means of exchange. Typically, a customer makes a withdrawal from his bank account and receives electronic coins from the bank. The customer can then use these coins to pay a merchant. The merchant can check the validity of the coins using cryptographic techniques. Then the merchant can deposit the coins at the bank. Some electronic coin systems may be used with multiple banks. An advantage of electronic coins is that they may be validated by cryptographic techniques, hence convincing merchants that these coins are indeed valid. However, a merchant has no way to determine on his own whether a coin has been spent before. In order to determine this, the coin has to be given to the bank and the bank has to check to see if that coin has been deposited previously. Some systems suggest the use of tamper resistant hardware for storing the coins such

that a tamper resistant component has to be broken in order for a customer to spend a coin more than once. Electronic coin systems may provide a very high degree of anonymity. Even if the banks and merchants pool their information about transactions, the identity of the payer of a particular transaction cannot be determined. Since the degree of anonymity might not be acceptable by some governments, there are also electronic coin payment systems that allow a payer's identity to be determined by trustees. These trustees would be typically independent of the banks and merchants. One problem with these electronic coin systems is that a single payment might require the use of multiple coins in order to total to the correct value. Electronic coin systems are designed to be used for offline systems, but can be used for online system as well. In such as case, the merchant would deposit the coins and receive a confirmation of the validity of the coins before providing merchandise. In fact, digital cash transactions are much like cash transactions. Payments are immediate and non-supplicated. Regardless of the provisions the issuer makes to protect against lost or damaged tokens, anonymity means the consumer will be vulnerable to loss. To protect against fraud and loss, some electronic coin systems serialize the tokens that they issue. If the consumer cannot produce a record of the serial numbers or if the tokens are redeemed by someone else, then the consumer has indeed lost the value that the tokens represent, their "cash" value, in effect. Anonymity imposes additional overhead on issuers because they must retain extensive records of serial numbers for tokens that they have issued.

Stored-Value Cards. Another approach to electronic payment uses devices that store a value in them. These devices contain a register that maintains an accounting of the value stored in the device. Typically, a customer connects with a bank through an

ATM or equivalent device and withdraws money from his bank account and the value of the withdrawal is added to the register in the device. The customer can authorize a movement of funds from his device to another device in the system. During this process, the value on his device is reduced and the value on the other device is increased by the same amount. In some systems, any device can accept payments. In other systems, only specified devices can accept payments. An advantage of the stored-value card is that it requires little processing at the bank. Transactions can take place with no involvement of the bank at all. A serious problem with stored-value devices is the possibility that a customer may fraudulently add value to his device. One method for reducing the risk of this is to limit the scope of acceptability of the devices. For example, a metropolitan transit system may provide cards that can only be used in the transit system. Another method for reducing risk is to design these devices such that they are extremely difficult to break into. However, this still leaves the stored-value device system vulnerable to attack. If these devices were to become widely used, it could become financially profitable for an attacker to break into one or more devices and record a large value in the device's register. If the system does not provide for the detection and recovery from such an attack, then the possibility of large losses is very real. In an alternative stored-value card system that is used offline, tamper resistant trusted devices are employed. In such a system, a device would have a signature key authorized by a bank. By taking the device to an ATM, or through an alternate means of communications with the bank, a customer may withdraw money from his bank account. In addition, the resulting balance is recorded in the device together with an identifying number that is unique to the particular withdrawal. Then, when the customer wants to pay a merchant, the device would use the signature key to

sign an order to pay the merchant for a specified amount. The balance recorded in the customer's device would then be debited by that amount and the balance recorded in the merchant's device would be credited by that amount. Typically, several balances may be maintained in the customer's device. One problem with this system is that it requires the bank to keep all the records corresponding to a particular withdrawal until the entire withdrawal has been accounted for. Since a transactions may involve many merchants, this problem is exacerbated as all of the corresponding records must be maintained until each merchant's device has been reconciled at an ATM. Another problem with this system is the need for a receiver to check all signatures for valid cash values if transactions pass through several hands. A further problem with this system is related to privacy in that the privacy of a given transaction is protected only by the security of the trusted device. Therefore, if this system were used for low value transactions with a correspondingly lower level of device security, privacy may be more easily compromised.

Electronic Script. Electronic script is a form of electronic currency in which a merchant is identified at the time of issuance of the currency such that the currency may only be spent in a transaction with the identified merchant. Typically, if a customer identifies a new merchant that he wishes to make a purchase from, or if a customer runs out of script with a previous merchant, then the customer would obtain script from a broker for a specified total amount that may be divided into discreet portions to pay each merchant. The payment to the broker for the script may involve another type of electronic payment. The customer may then make payments to the specified merchant until the total is reached or until the customer does not want to make any more payments to that merchant during a given time period. Subsequently,

the merchant must deposit the script with the broker. The broker then pays the merchant through some other payment mechanism. Since this system uses another electronic payment system for the customer to purchase scripts from the broker and for the broker to pay the merchant for a redeemed script, it is most useful in situations where a customer has many transactions with a single merchant. In such circumstances, it is more efficient than other electronic payment systems because of the reduced computational complexity that is typically required for a script payment.

The problem with the debit systems, credit card based systems, electronic check systems, electronic coin systems, stored-value card systems, and electronic script systems discussed above is that they require the maintenance of extensive records, they do not provide a high level of anonymity for consumers, and their processing costs are too high such that they cannot adequately facilitate micro payments to individual merchants. As mentioned above, micro payments are very low value payments that typically occur in high volumes on digital communication networks. For example, a stockbroker may wish to sell stock quotes at $0.01US per quote over the Internet. In such a case, while the cost per sale item is very low, the number of items sold per day may be very high. In addition, for credit card or check-based payment systems, the recipient or the system provider must assume some credit risk as a buyer may be denied or may be unable to pay. Insurance fees related to this assumed risk raise the cost of the payment service. With respect to anonymity, this feature is becoming more essential to consumers as it is possible, according to privacy advocates, to collect and analyze large amounts of data concerning every purchase or road toll payment that a consumer makes which in turn raises potential privacy problems. Finally, with respect to payment systems where instantaneous payments are

made to merchants, a problem exists in that fraud detection may occur too late. For example, if a merchant accepts a fraudulent transaction, the transaction may not be detected until after the merchant receives the money.

A need therefor exists for an electronic payment method and system that is non-supplicated, that does not require the maintenance of extensive records, that is relatively anonymous for the consumer, that can detect fraud, and that can adequately deal with micro payments to individual merchants. The required payment system and method should include general features such as high performance, low cost, minimum maintenance, scalability according to volume, significant security with moderate anonymity and strong authentication, standards based with an open architecture, and adaptable discrepancy detection.

In general, online transactions are currently made over a network connection between a customer and a transaction enabled merchant server. The customer proceeds through the steps of selecting products and services and then making final decisions with respect to the purchase of these selected products and services. Typically these steps are referred to as "adding to a shopping cart" and "checking out". The process itself may be referred to as the "shopping phase". Upon completion of the shopping phase, the merchant server will require a payment commitment. This payment commitment is required to proceed with fulfillment of the customer's order. It is at this stage that some means of authenticating the buyer and binding the identity of the buyer to the transaction is required. As such, authentication is the primary hurdle between non-consummated transactions and true online commerce.

Now, smart cards typically employ integrated circuitry and programmable microprocessors in a credit card sized format that includes external contacts for interfacing with other devices. The interface devices may include sales terminals, automated teller machines, and other similar computer integrated devices. As discussed above, smart cards are deployed in several financial applications including stored-value, credit and debit, and loyalty point environments. These applications require the card to maintain some means of content integrity, whether for the monetary value stored on the card, for identity information, or for financial data. In several currently available smart card systems, a means of hardware encryption is imbedded into the cards' integrated circuitry or is contained in accompanying interface software.

For example, a smart card may have financial credit information contained in a chip enabled secure token. A point of sale terminal associated with the system securely extracts the relevant data from the smart card at the time of purchase and transmits this data over a secured channel to a payment processor. In such a system, the transaction may only be validated as long as the token is present and in contact with the sales terminal. Upon withdrawal of the token, the security protocol is breached and financial transactions are inhibited. As an alternative, a stored-value card may be used in this system such that the financial transaction takes place by downloading a value amount from the card to the sales terminal. In either case, transaction data may be subsequently sent in aggregate by the sales terminal to a payment processing system in batch. Finally, the payment processor will transfer funds between the appropriate agents for the buyer and the seller.

Typically, these systems require the physical presence of the card, the buyer, the sales terminal, and quite often the actual goods to be purchased. An advantage of these systems is that a degree of authentication is provided by the physical presence of the customer in the company of the merchant and the sales terminal. However, physical presence is not available in a remote e-commerce environment. In such an environment, the buyer's terminal typically connects with a merchant server over an open network. As such, the identity of the person in possession of the smart card is based on very weak authentication. Furthermore, the distributed nature of these systems lends itself to the loss or theft of the physical token that limits the ability of the buyer to access their online financial persona.

The nature of smart card technology requires that information be recorded on the card. In the case of stored-value cards, a monetary amount must be downloaded to the card. In the case of a debit or credit cards, an identity must be securely transferred to the card. Hence, a need exists in electronic commerce systems for a method of online authentication that will include the benefits of physical smart card technology in a virtual environment. In addition, a need exists for an electronic commerce system that provides the benefits of card present transactions in the context of a remote network environment. Furthermore, a need exists for an electronic commerce system that will reduce the costs incurred by current card technology associated with card distribution, reader distribution, and connectivity. Moreover, a need exists for an electronic commerce system that includes adequate authentication and security provisions.

It is an object of the present invention to provide for at least some of the above-mentioned needs. It is a further object of the present invention to obviate or mitigate at least some of the above-mentioned problems and disadvantages.

SUMMARY OF THE INVENTION

The invention provides a method and system for electronic commerce involving virtual smart cards and virtual safes. The method and system is entitled "VirtualSAFE".

According to one aspect of the invention, a method for electronic commerce is provided.

According to another aspect of the invention, a data processing system is provided. This data processing system has stored therein data representing sequences of instructions which when executed cause the above method to be performed. The data processing system generally includes servers, clients, Internet access, databases, and VirtualSAFE software.

According to another aspect of the invention, a system and method is provided that is comprised of a remote multi-tiered Authentication Authority ("AA") infrastructure that enables extremely powerful security functions when processing electronic data and transactions over conventional and wireless networks, authenticating users at the application, network access, transaction and communications layers.

According to another aspect of the invention, a system and method is provided for payment and initiation using a computer network. Specifically, the present invention relates to a payment and initiation system for a virtual smart card using an open network like the Internet.

According to another aspect of the invention, a system and method is provided that consists of highly secure dedicated servers. Built upon a "need to know virtual identity" principle of access, the system and method securely processes and stores information such that only an authorized user who is vigorously and firmly authenticated can access it. While the secure session and/or the SSL protocol authenticates and secures communications with the server, and Public Key Infrastructure (PKI) combined with third party trusted Certificate Authorities authenticates the device or computer, the VirtualSAFE system and method authenticates the server, computer, and the user.

According to another aspect of the invention, a system and method is provided wherein using a PKI-based secure application, an enrolling applicant is prompted to store personal information to a VirtualSAFE remote repository. The depositing of information is a unique process. It involves encrypting the information with a PKI cryptographic scheme that uses a high-speed hybrid approach, and then storing elements of it in a fragmented arrangement. Only the authenticated user can bring these pieces together again to render the information usable. In this process, the user profile becomes a virtual safety deposit box or part of a "virtual identity", the contents of which are accessible only to VirtualSAFE for the purpose of authentication, and only in the online presence of the authorized user. The secure data is not accessible to any entity or application requesting user authentication, or to VirtualSAFE administrators.

According to another aspect of the invention, a system and method is provided wherein user identity authentication is initiated for each individual transaction by

triggering a multi-tiered algorithm that employs "virtual smart card" technology to interface with standard PKI. Authentication is only possible when the user's personalized "virtual smart card" allows VirtualSAFE to access the respective "virtual identity".

According to another aspect of the invention, a system and method is provided that may be applied to credit or debit card, safe check, wire, or other forms of electronic payment processing.

According to another aspect of the invention, a system and method is provided that applies equally as a means of network access control and secure data storage.

According to another aspect of the invention, a system and method is provided that, over a remote network, is configured as an Attribute Authentication Authority ("AAA") and provides an access control portal to sensitive applications and data management facilities hence enabling a secure end-to-end extranet for maintaining authorization, authentication, and accountability of all external users or applications. Strong user and/or application authentication via virtual smart card directs, controls, and audits access to sensitive resources to any level of granularity in accordance with the ISO 8583 standard.

According to another aspect of the invention, a system and method is provided for the complete payment and fulfillment process as conducted over a communication network, and more specifically, the system and method provides a secure virtual entity that includes purchase transaction, payment transaction, and shipping and delivery components.

According to another aspect of the invention, a system and method is provided which executes a complete electronic financial transaction for goods or services, which previously was transacted with credit card, cash or other payment of goods, and subsequently fulfilled separately.

According to another aspect of the invention, a system and method is provided wherein by enabling an unprecedented level of security in online authentication, the VirtualSAFE system and method eliminates the current constraints on businesses, governments, and individuals that keep them from fully leveraging the flexibility and advantages of communicating and transacting over the Internet, intranets, extranets and enterprise networks. This is made possible by VirtualSAFE's multi-tiered Attribute Authentication Authority (AAA) infrastructure which includes secure means for processing electronic data and transactions over conventional and wireless networks, authenticating users at the application level, and for network access, transactions, and communications.

According to another aspect of the invention, a system and method is provided that includes highly secure, dedicated server technology that exceeds standard sessions or Internet security protocols such as SSL. While SSL authenticates a network server and Public Key Infrastructure (PKI) combined with third party trusted Certificate Authorities authenticate the device or PC, VirtualSAFE authenticates the user.

According to another aspect of the invention, a system and method is provided for the payment and fulfillment processes involved in completing a financial exchange of goods or services for monetary payment. The electronic process for implementing money payments and delivery is an alternative medium of economic exchange to

cash, checks, credit and debit cards, wire payment, and electronic funds transfer over an open network.

According to another aspect of the invention, a system and method is provided that is a hybrid of secure encrypted digital communications, existing payment methods (i.e. cash, check, credit and debit card payment systems, wire payment and electronic funds transfer systems, etc.), and fulfillment and clearinghouse processes for delivery of goods and services. The invention possesses many of the benefits of these systems with few of their limitations. The invention uses electronic representations of money and shopping entities which are designed to be securely housed in a digital environment that is independent from the remote shopper's computer terminal.

According to another aspect of the invention, a system and method is provided that enables an enterprise to resolve the security, privacy, convenience and cost impediments that exist with online commerce.

According to another aspect of the invention, a system and method is provided that makes it exceptionally easy and virtually risk-free for businesses of all sizes to engage in e-commerce. The invention accomplishes this by providing technology and relationships to online buyers and merchants that creates a frictionless transaction environment.

According to another aspect of the invention, a system and method is provided that ensures user customer satisfaction in the following areas: E-Commerce Transactions over the internet (ECToIP); Guaranteed Secure Communications protocol (GSC); and, Secured Storage Virtual Facilities and Repository (SSVFP).

According to another aspect of the invention, a system and method is provided that makes it exceeding easy for potential online merchants of goods and services to build a website and enter the world of e-commerce.

According to another aspect of the invention, a system and method is provided which allows merchants to readily obtain blanket fraud insurance.

According to another aspect of the invention, a system and method is provided that combines a number of technologies that in turn are based on the public key infrastructure (PKI). This combination of technologies is what makes VirtualSAFE unique. The technology enables VirtualSAFE to register consumers' personal data (i.e. credit card information) once and then issue a digital ID to that individual. Henceforth the consumer never has to enter their data online again, an obvious attraction to consumers. The data is then held in a database file on a highly secure and insured server site.

According to another aspect of the invention, a system and method is provided wherein all parts of a transaction are routed through a "safe" component, with private data being protected. A purchase can then be made with all interested parties (i.e. merchant, credit card issuer, bank, couriers) accessing only information that is absolutely pertinent to their roles. At the same time, the invention ensures that it is exceedingly unlikely that anyone other than the card holder could execute the transaction. An advantage of VirtualSAFE is that online fraud may be reduced by at least 90%.

According to another aspect of the invention, a system and method is provided that combines security, privacy, and ease of use in a manner that is unique in the realm of e-commerce.

According to another aspect of the invention, a system and method is provided that includes a remote secure repository for fulfillment data.

According to another aspect of the invention, a system and method is provided that electronically emulates a wallet or a purse customarily used for organizing money, credit cards, and other forms of payment. Access to the instruments in the wallet or purse is restricted by a sophisticated encryption and authentication method to avoid unauthorized payments. A successful cryptographic authentication is required in order to obtain access to the wallet or purse. The authentication protocol obtains the information necessary for creating a network session granting authority to utilize an instrument, a payment holder, and a complete electronic wallet. Electronic approval results in the generation of an electronic transaction to complete the order.

According to another aspect of the invention, a system and method is provided wherein upon selection of a particular payment transaction by a user, a particular transaction notification will be generated based on the order. The transaction notification is processed by means of a secure connection to a transaction server. The transaction server consists of the required elements for order fulfillment, including connectivity to: credit card issuer, acquiring bank or funds-holding institution, product or service merchant, delivery provider, and the user or customer account.

According to another aspect of the invention, a system and method is provided wherein an electronic payment transaction is generated in a computer-based method for affecting a transfer of funds from an account of the payer in the funds-holding institution to the payee. The electronic instrument includes a cryptographic digital signature of the payer, digital representations of payment instructions, the cryptographic authenticated identity of the payer, the identity of the payee, and the identity of the funds-holding institution.

According to another aspect of the invention, a system and method is provided that has a secure infrastructure which includes the following components: PKI; a Redirection Link; a Secure Remote Pointer/Plug-In Application; a Virtual Identity; a Virtual Smart Card; a VirtualSAFE Deposit Box (VSDB); an Attribute Authority; a Crypto-Engine; a Payment Processing Engine; a Risk Management Engine; a Transaction Fulfilment Mechanism; an Insurance Module; and, a Transaction Secure Repository.

According to another aspect of the invention, a system and method is provided that augments the existing capabilities to process payments by simulating the nature of a physical smart card, reader, and unique identity in a remote online environment. This is accomplished by the invention without compromising existing capabilities of remote connection, browsing, and interactivity already inherent in the network. These exisitng capabilities are enhanced by the invention's ability to strongly authenticate the identity of online users for the purposes of processing payments.

According to another aspect of the invention, a system and method is provided which, by incorporating cryptographic and networking elements, operates as an

authentication layer or authentication authority between the buyer, the terminal, the merchant, and payment server. Through multi-tiered authentication technology, the remote client is queried and authenticated to produce effective smart card emulation as if the physical card was present. The advantages to such a cryptographically enabled virtual scheme over a distributed smart card infrastructure are great. The nature of the physical smart card requires initialization criteria to be met before a transaction may actually take place. Initialization criteria often include pre-initiation of the smart card with stored-values of monetary amounts, financial data, or identification data. Furthermore, beyond initialization, re-configuration of data on the card may have to be performed frequently, for example, where personal or financial data is involved.

According to another aspect of the invention, a system and method is provided which includes an online purchase and initiation server (VirtualSAFE Authentication Authority or "VSAA") that implements virtual smart cards. The present invention complements existing Internet payment and initiation systems by providing software emulation of smart cards and smart card readers. Other components of the existing Internet payment and initiation systems (e.g. merchant server and payment server), and the techniques for processing payment and initiation transactions, may remain the same. Use of the VSAA server is transparent to merchants on the Internet. In one embodiment, a smart card and its associated card reader are emulated on a remotely located VSAA server computer, thus deterring the need for physical smart cards and smart card readers. The existing client terminal acts as a pass-through device that is transparent to a user, a merchant server, or a bank server. This enhancement to Internet payment and initiation systems provides many advantages. For example, the

invention accelerates the adoption of electronic market systems by avoiding the cost and distribution problems associated with physical cards and card readers. When infrastructure to support physical smart cards and card readers is developed, a further advantage of the invention is that it functionality may be replaced using a hardware approach or it may be used in conjunction with the actual hardware.

According to another aspect of the invention, a system and method is provided that includes a mechanism to address the low value (less then $10.00US) electronic commerce market in a rapid manner using an infrastructure that is easily scaleable.

According to another aspect of the invention, a system and method is provided that, by remaining integrated with the hardware-based approach to electronic commerce, facilitates the accelerated development of Internet payment and initiation systems. With the invention, a base of consumers may be created which may subsequently be transferred to the hardware approach when the required hardware is more widely available.

According to another aspect of the invention, a system and method is provided that is secure in that the cryptographic functions normally performed within a smart card are performed securely within the remote VSAA server which may be under the control of an issuing bank or a trusted third party.

According to another aspect of the invention, a system and method is provided with the advantage that value may be credited to a consumer's account. This may be done quickly and easily by the invention's VSAA server (i.e. the virtual smart card that is

being emulated). A special initiation server is not necessarily required, but may be used.

According to another aspect of the invention, a system and method is provided wherein, with the invention's VSAA server, use of a virtual smart card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant, dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for a small dollar amount transaction because of the service fees per transaction. By permitting the use of a virtual card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and services that he provided for free in the past. The invention is suitable for purchases of under $10.00US while purchases of any amount may be made. The invention allows merchants to recover costs of services not previously charged for and allows merchants to access to an existing and rapidly growing consumer base.

According to another aspect of the invention, a system and method is provided that integrates into an existing clearing and settlement system such that merchants need not implement nor become familiar with new procedures for reconciliation of transactions.

According to another aspect of the invention, a system and method is provided with the advantage that a merchant need only make a minimal investment in time and money to take advantage of and to accept payments over the Internet. With the

invention, a merchant need not engage in the development of complex software or accounting procedures. Smaller merchants will especially benefit from the invention. By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and services from his web site. Since a virtual smart card with a stored-value application is used, the payment server and the VSAA server perform the details of and provide security for the transaction. Hence, merchants are relieved from having to control and keep track of transactions. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a card nor for determining a balance on the card.

According to another aspect of the invention, a system and method is provided that, in one embodiment, facilitates frequent flyer miles or award points. A consumer may wish to access any of a variety of Web servers in order to redeem frequent flyer miles, award points, etc., that he or she has accumulated as part of a loyalty program. The consumer may have accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication company, etc. Often the consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. It is important to the airline (or other company) to be able to authenticate that the person trying to redeem points is the actual person who owns the points. By accessing a Web server associated with the

particular program, an embodiment of the invention allows the consumer to use a virtual card in the VSAA server to authenticate that he or she is the true owner of the points and to receive benefits from the program.

According to another aspect of the invention, a system and method is provided that, in one embodiment, allows consumer to conveniently initiate value on virtual cards from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office, or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's virtual card. At the same time, the corresponding value is transferred from the bank to the virtual card issuer through existing networks for later settlement with a merchant from whom the consumer purchases goods or services. This embodiment makes use of an existing clearing and settlement system for eventual settlement of the transaction between the merchant and the card issuer. The invention allows consumers to conveniently initiate value on virtual cards while maintaining a high level of security. From the consumer's perspective, this initiation feature operates in a fashion similar to the initiation of a physical card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor is the consumer required to travel to a bank. The initiation functionality is distributed across the Internet between the VSAA server, a bank server holding the consumer's account, and an initiation server with a security module. All of these entities may be physically remote from one another with router functionality being provided by the Internet.

According to another aspect of the invention, a system and method is provided that may use existing clearing and settlement systems to reconcile transactions and to pay the appropriate parties once the value has been spent. A new system and methodology for reconciling transactions need not be developed or implemented. By using existing clearing and settlement systems, the implementation of the invention is simplified. In addition, a participating bank, for example, need not implement or become familiar with new procedures for reconciliation of transactions.

According to another aspect of the invention, a system and method is provided that includes the integration of four separate networks, namely, "VIRCON", "VIRSBUS", "VIRMBUS", and "VIRLBUS". These networks are defined as follows: VIRCON is a virtual contractors network; VIRSBUS is a virtual small business network; VIRMBUS is a virtual medium-sized business network; and, VIRLBUS is a virtual large business network. As members of one these networks, contractors will have access and will be able to run all of their business affairs via VirtualSAFE. Contractors may login to VirtualSAFE and download all of their companys' documents (e.g. purchase orders, invoices, change orders, material order forms, outstanding bills, etc.) and have all of their e-commerce transactions handled right at their customers' sites. For materials that they require, emails will be sent to their suppliers. For invoices that require payment, the opportunity for their immediate payment exists through VirtualSAFE.

According to another aspect of the invention, a system and method is provided that includes a check processing module, namely, "SAFEcheck". With SAFEcheck, check printers are installed in participating banks or other financial institutions enabling

employees of participating corporate members of VirtualSAFE to print out their paychecks at these locations. SAFEcheck alleviates many of the problems associated with checks being lost in the mail.

According to another aspect of the invention, a method and system is provided that supports multiple languages.

According to another aspect of the invention, a method and system is provided that supports multiple currencies.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by referring to the following description and accompanying drawings which illustrate the invention. In the drawings:

FIG. 1 is a block diagram illustrating the components of the VirtualSAFE method and system in accordance with the preferred embodiment;

FIG. 2 is a block diagram illustrating the secure remote pointer component of the VirtualSAFE method and system in accordance with the preferred embodiment;

FIG. 3 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in the general case in accordance with the preferred embodiment;

FIG. 4 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a second case in accordance with the preferred embodiment;

FIG. 5 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a third case in accordance with the preferred embodiment;

FIG. 6 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a fourth case in accordance with the preferred embodiment;

FIG. 7 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a fifth case in accordance with the preferred embodiment;

FIG. 8 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a sixth case in accordance with the preferred embodiment;

FIG. 9 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a seventh case in accordance with the preferred embodiment;

FIG. 10 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in an eighth case in accordance with the preferred embodiment;

FIG. 11 is a flowchart illustrating the steps for user enrollment in VirtualSAFE in a ninth case in accordance with the preferred embodiment;

FIG. 12 is a flowchart illustrating CA processes in VirtualSAFE in accordance with the preferred embodiment;

FIG. 13 is a block diagram illustrating the participants and their contractual relationships in VirtualSAFE in accordance with the preferred embodiment;

FIG. 14 is a block diagram illustrating the enrollment process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 15 is a block diagram illustrating the online transaction process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 16 is a block diagram illustrating the server authentication process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 17 is a block diagram illustrating the computer authentication process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 18 is a block diagram illustrating the user authentication process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 19 is a block diagram illustrating the back-end authentication process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 20 is a block diagram illustrating the fulfillment process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 21 is a block diagram illustrating the attribute authentication authority process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 22 is a block diagram illustrating the virtual identity (VI) process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 23 is a block diagram illustrating the virtual smart card (VSC) process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 24 is a block diagram illustrating the VirtualSAFE deposit box (VSDB) process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 25 is a block diagram illustrating the point-of-sale (POS) and virtual smart card (VSC) emulation process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 26 is a block diagram illustrating the ATM and virtual smart card (VSC) emulation process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 27 is a block diagram illustrating the wireless POS and ATM process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 28 is a block diagram illustrating the SAFEcheck process in VirtualSAFE in accordance with the preferred embodiment;

FIG. 29 is a block diagram illustrating physical access control in VirtualSAFE in accordance with the preferred embodiment;

FIG. 30 is a block diagram illustrating the overall VirtualSAFE method and system, from a business to business perspective and including an e-portal, in accordance with the preferred embodiment; and,

FIG. 31 is a block diagram illustrating the overall VirtualSAFE method and system, from a business to consumer perspective and including a merchant, in accordance with the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances, well-known software, circuits, structures and techniques have not been described or shown in detail in order not to obscure the invention. The term data processing system is used herein to refer to any machine for processing data, including the computer systems and network arrangements described herein. The term "VirtualSAFE" is used herein to refer to the method and system of the invention including associated software. The method and system described herein is applicable to electronic commerce.

According to one aspect of the invention, a method for electronic commerce is provided.

According to another aspect of the invention, a data processing system is provided. This data processing system has stored therein data representing sequences of instructions which when executed cause the above method to be performed. The data processing system generally includes servers, clients, Internet access, databases, and VirtualSAFE software.

According to another aspect of the invention, a system and method is provided that is comprised of a remote multi-tiered Authentication Authority ("AA") infrastructure that enables extremely powerful security functions when processing electronic data and transactions over conventional and wireless networks, authenticating users at the application, network access, transaction and communications layers.

According to another aspect of the invention, a system and method is provided for payment and initiation using a computer network. Specifically, the present invention relates to a payment and initiation system for a virtual smart card using an open network like the Internet.

According to another aspect of the invention, a system and method is provided that consists of highly secure dedicated servers. Built upon a "need to know virtual identity" principle of access, the system and method securely processes and stores information such that only an authorized user who is vigorously and firmly authenticated can access it. While the secure session and/or the SSL protocol authenticates and secures communications with the server, and Public Key Infrastructure (PKI) combined with third party trusted Certificate Authorities authenticates the device or computer, the VirtualSAFE system and method authenticates the server, computer, and the user.

According to another aspect of the invention, a system and method is provided wherein using a PKI-based secure application, an enrolling applicant is prompted to store personal information to a VirtualSAFE remote repository. The depositing of information is a unique process. It involves encrypting the information with a PKI cryptographic scheme that uses a high-speed hybrid approach, and then storing elements of it in a fragmented arrangement. Only the authenticated user can bring these pieces together again to render the information usable. In this process, the user profile becomes a virtual safety deposit box or part of a "virtual identity", the contents of which are accessible only to VirtualSAFE for the purpose of authentication, and only in the online presence of the authorized user. The secure data is not accessible to

any entity or application requesting user authentication, or to VirtualSAFE administrators.

According to another aspect of the invention, a system and method is provided wherein user identity authentication is initiated for each individual transaction by triggering a multi-tiered algorithm that employs "virtual smart card" technology to interface with standard PKI. Authentication is only possible when the user's personalized "virtual smart card" allows VirtualSAFE to access the respective "virtual identity".

According to another aspect of the invention, a system and method is provided that may be applied to credit or debit card, safe check, wire, or other forms of electronic payment processing.

According to another aspect of the invention, a system and method is provided that applies equally as a means of network access control and secure data storage.

According to another aspect of the invention, a system and method is provided that, over a remote network, is configured as an Attribute Authentication Authority ("AAA") and provides an access control portal to sensitive applications and data management facilities hence enabling a secure end-to-end extranet for maintaining authorization, authentication, and accountability of all external users or applications. Strong user and/or application authentication via virtual smart card directs, controls, and audits access to sensitive resources to any level of granularity in accordance with the ISO 8583 standard.

According to another aspect of the invention, a system and method is provided for the complete payment and fulfillment process as conducted over a communication network, and more specifically, the system and method provides a secure virtual entity that includes purchase transaction, payment transaction, and shipping and delivery components.

According to another aspect of the invention, a system and method is provided which executes a complete electronic financial transaction for goods or services, which previously was transacted with credit card, cash or other payment of goods, and subsequently fulfilled separately.

According to another aspect of the invention, a system and method is provided wherein by enabling an unprecedented level of security in online authentication, the VirtualSAFE system and method eliminates the current constraints on businesses, governments, and individuals that keep them from fully leveraging the flexibility and advantages of communicating and transacting over the Internet, intranets, extranets and enterprise networks. This is made possible by VirtualSAFE's multi-tiered Attribute Authentication Authority (AAA) infrastructure which includes secure means for processing electronic data and transactions over conventional and wireless networks, authenticating users at the application level, and for network access, transactions, and communications.

According to another aspect of the invention, a system and method is provided that includes highly secure, dedicated server technology that exceeds standard sessions or Internet security protocols such as SSL. While SSL authenticates a network server

and Public Key Infrastructure (PKI) combined with third party trusted Certificate Authorities authenticate the device or PC, VirtualSAFE authenticates the user.

According to another aspect of the invention, a system and method is provided for the payment and fulfillment processes involved in completing a financial exchange of goods or services for monetary payment. The electronic process for implementing money payments and delivery is an alternative medium of economic exchange to cash, checks, credit and debit cards, wire payment, and electronic funds transfer over an open network.

According to another aspect of the invention, a system and method is provided that is a hybrid of secure encrypted digital communications, existing payment methods (i.e. cash, check, credit and debit card payment systems, wire payment and electronic funds transfer systems, etc.), and fulfillment and clearinghouse processes for delivery of goods and services. The invention possesses many of the benefits of these systems with few of their limitations. The invention uses electronic representations of money and shopping entities which are designed to be securely housed in a digital environment that is independent from the remote shopper's computer terminal.

According to another aspect of the invention, a system and method is provided that enables an enterprise to resolve the security, privacy, convenience and cost impediments that exist with online commerce.

According to another aspect of the invention, a system and method is provided that makes it exceptionally easy and virtually risk-free for businesses of all sizes to engage in e-commerce. The invention accomplishes this by providing technology and

relationships to online buyers and merchants that creates a frictionless transaction environment.

According to another aspect of the invention, a system and method is provided that ensures user customer satisfaction in the following areas: E-Commerce Transactions over the internet (ECToIP); Guaranteed Secure Communications protocol (GSC); and, Secured Storage Virtual Facilities and Repository (SSVFP).

According to another aspect of the invention, a system and method is provided that makes it exceeding easy for potential online merchants of goods and services to build a website and enter the world of e-commerce.

According to another aspect of the invention, a system and method is provided which allows merchants to readily obtain blanket fraud insurance.

According to another aspect of the invention, a system and method is provided that combines a number of technologies that in turn are based on the public key infrastructure (PKI). This combination of technologies is what makes VirtualSAFE unique. The technology enables VirtualSAFE to register consumers' personal data (i.e. credit card information) once and then issue a digital ID to that individual. Henceforth the consumer never has to enter their data online again, an obvious attraction to consumers. The data is then held in a database file on a highly secure and insured server site.

According to another aspect of the invention, a system and method is provided wherein all parts of a transaction are routed through a "safe" component, with private data being protected. A purchase can then be made with all interested parties (i.e.

merchant, credit card issuer, bank, couriers) accessing only information that is absolutely pertinent to their roles. At the same time, the invention ensures that it is exceedingly unlikely that anyone other than the card holder could execute the transaction. An advantage of VirtualSAFE is that online fraud may be reduced by at least 90%.

According to another aspect of the invention, a system and method is provided that combines security, privacy, and ease of use in a manner that is unique in the realm of e-commerce.

According to another aspect of the invention, a system and method is provided that includes a remote secure repository for fulfillment data.

According to another aspect of the invention, a system and method is provided that electronically emulates a wallet or a purse customarily used for organizing money, credit cards, and other forms of payment. Access to the instruments in the wallet or purse is restricted by a sophisticated encryption and authentication method to avoid unauthorized payments. A successful cryptographic authentication is required in order to obtain access to the wallet or purse. The authentication protocol obtains the information necessary for creating a network session granting authority to utilize an instrument, a payment holder, and a complete electronic wallet. Electronic approval results in the generation of an electronic transaction to complete the order.

According to another aspect of the invention, a system and method is provided wherein upon selection of a particular payment transaction by a user, a particular transaction notification will be generated based on the order. The transaction

notification is processed by means of a secure connection to a transaction server. The transaction server consists of the required elements for order fulfillment, including connectivity to: credit card issuer, acquiring bank or funds-holding institution, product or service merchant, delivery provider, and the user or customer account.

According to another aspect of the invention, a system and method is provided wherein an electronic payment transaction is generated in a computer-based method for affecting a transfer of funds from an account of the payer in the funds-holding institution to the payee. The electronic instrument includes a cryptographic digital signature of the payer, digital representations of payment instructions, the cryptographic authenticated identity of the payer, the identity of the payee, and the identity of the funds-holding institution.

According to another aspect of the invention, a system and method is provided that has a secure infrastructure which includes the following components: PKI; a Redirection Link; a Secure Remote Pointer/Plug-In Application; a Virtual Identity; a Virtual Smart Card; a VirtualSAFE Deposit Box (VSDB); an Attribute Authority; a Crypto-Engine; a Payment Processing Engine; a Risk Management Engine; a Transaction Fulfilment Mechanism; an Insurance Module; and, a Transaction Secure Repository.

According to another aspect of the invention, a system and method is provided that augments the existing capabilities to process payments by simulating the nature of a physical smart card, reader, and unique identity in a remote online environment. This is accomplished by the invention without compromising existing capabilities of remote connection, browsing, and interactivity already inherent in the network. These

exisitng capabilities are enhanced by the invention's ability to strongly authenticate the identity of online users for the purposes of processing payments.

According to another aspect of the invention, a system and method is provided which, by incorporating cryptographic and networking elements, operates as an authentication layer or authentication authority between the buyer, the terminal, the merchant, and payment server. Through multi-tiered authentication technology, the remote client is queried and authenticated to produce effective smart card emulation as if the physical card was present. The advantages to such a cryptographically enabled virtual scheme over a distributed smart card infrastructure are great. The nature of the physical smart card requires initialization criteria to be met before a transaction may actually take place. Initialization criteria often include pre-initiation of the smart card with stored-values of monetary amounts, financial data, or identification data. Furthermore, beyond initialization, re-configuration of data on the card may have to be performed frequently, for example, where personal or financial data is involved.

According to another aspect of the invention, a system and method is provided which includes an online purchase and initiation server (VirtualSAFE Authentication Authority or "VSAA") that implements virtual smart cards. The present invention complements existing Internet payment and initiation systems by providing software emulation of smart cards and smart card readers. Other components of the existing Internet payment and initiation systems (e.g. merchant server and payment server), and the techniques for processing payment and initiation transactions, may remain the same. Use of the VSAA server is transparent to merchants on the Internet. In one

embodiment, a smart card and its associated card reader are emulated on a remotely located VSAA server computer, thus deterring the need for physical smart cards and smart card readers. The existing client terminal acts as a pass-through device that is transparent to a user, a merchant server, or a bank server. This enhancement to Internet payment and initiation systems provides many advantages. For example, the invention accelerates the adoption of electronic market systems by avoiding the cost and distribution problems associated with physical cards and card readers. When infrastructure to support physical smart cards and card readers is developed, a further advantage of the invention is that it functionality may be replaced using a hardware approach or it may be used in conjunction with the actual hardware.

According to another aspect of the invention, a system and method is provided that includes a mechanism to address the low value (less then $10.00US) electronic commerce market in a rapid manner using an infrastructure that is easily scaleable.

According to another aspect of the invention, a system and method is provided that, by remaining integrated with the hardware-based approach to electronic commerce, facilitates the accelerated development of Internet payment and initiation systems. With the invention, a base of consumers may be created which may subsequently be transferred to the hardware approach when the required hardware is more widely available.

According to another aspect of the invention, a system and method is provided that is secure in that the cryptographic functions normally performed within a smart card are performed securely within the remote VSAA server which may be under the control of an issuing bank or a trusted third party.

According to another aspect of the invention, a system and method is provided with the advantage that value may be credited to a consumer's account. This may be done quickly and easily by the invention's VSAA server (i.e. the virtual smart card that is being emulated). A special initiation server is not necessarily required, but may be used.

According to another aspect of the invention, a system and method is provided wherein, with the invention's VSAA server, use of a virtual smart card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant, dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for a small dollar amount transaction because of the service fees per transaction. By permitting the use of a virtual card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and services that he provided for free in the past. The invention is suitable for purchases of under $10.00US while purchases of any amount may be made. The invention allows merchants to recover costs of services not previously charged for and allows merchants to access to an existing and rapidly growing consumer base.

According to another aspect of the invention, a system and method is provided that integrates into an existing clearing and settlement system such that merchants need not implement nor become familiar with new procedures for reconciliation of transactions.

According to another aspect of the invention, a system and method is provided with the advantage that a merchant need only make a minimal investment in time and money to take advantage of and to accept payments over the Internet. With the invention, a merchant need not engage in the development of complex software or accounting procedures. Smaller merchants will especially benefit from the invention. By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and services from his web site. Since a virtual smart card with a stored-value application is used, the payment server and the VSAA server perform the details of and provide security for the transaction. Hence, merchants are relieved from having to control and keep track of transactions. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a card nor for determining a balance on the card.

According to another aspect of the invention, a system and method is provided that, in one embodiment, facilitates frequent flyer miles or award points. A consumer may wish to access any of a variety of Web servers in order to redeem frequent flyer miles, award points, etc., that he or she has accumulated as part of a loyalty program. The consumer may have accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication company, etc. Often the consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays,

prizes, awards, discounts, or other benefits. It is important to the airline (or other company) to be able to authenticate that the person trying to redeem points is the actual person who owns the points. By accessing a Web server associated with the particular program, an embodiment of the invention allows the consumer to use a virtual card in the VSAA server to authenticate that he or she is the true owner of the points and to receive benefits from the program.

According to another aspect of the invention, a system and method is provided that, in one embodiment, allows consumer to conveniently initiate value on virtual cards from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office, or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's virtual card. At the same time, the corresponding value is transferred from the bank to the virtual card issuer through existing networks for later settlement with a merchant from whom the consumer purchases goods or services. This embodiment makes use of an existing clearing and settlement system for eventual settlement of the transaction between the merchant and the card issuer. The invention allows consumers to conveniently initiate value on virtual cards while maintaining a high level of security. From the consumer's perspective, this initiation feature operates in a fashion similar to the initiation of a physical card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor is the consumer required to travel to a bank. The initiation functionality is distributed across the Internet between the VSAA server, a bank server holding the consumer's account, and an initiation server with a security

module. All of these entities may be physically remote from one another with router functionality being provided by the Internet.

According to another aspect of the invention, a system and method is provided that may use existing clearing and settlement systems to reconcile transactions and to pay the appropriate parties once the value has been spent. A new system and methodology for reconciling transactions need not be developed or implemented. By using existing clearing and settlement systems, the implementation of the invention is simplified. In addition, a participating bank, for example, need not implement or become familiar with new procedures for reconciliation of transactions.

According to another aspect of the invention, a system and method is provided that includes the integration of four separate networks, namely, "VIRCON", "VIRSBUS", "VIRMBUS", and "VIRLBUS". These networks are defined as follows: VIRCON is a virtual contractors network; VIRSBUS is a virtual small business network; VIRMBUS is a virtual medium-sized business network; and, VIRLBUS is a virtual large business network. As members of one these networks, contractors will have access and will be able to run all of their business affairs via VirtualSAFE. Contractors may login to VirtualSAFE and download all of their companys' documents (e.g. purchase orders, invoices, change orders, material order forms, outstanding bills, etc.) and have all of their e-commerce transactions handled right at their customers' sites. For materials that they require, emails will be sent to their suppliers. For invoices that require payment, the opportunity for their immediate payment exists through VirtualSAFE.

According to another aspect of the invention, a system and method is provided that includes a check processing module, namely, "SAFEcheck". With SAFEcheck, check printers are installed in participating banks or other financial institutions enabling employees of participating corporate members of VirtualSAFE to print out their paychecks at these locations. SAFEcheck alleviates many of the problems associated with checks being lost in the mail.

According to another aspect of the invention, a method and system is provided that supports multiple languages.

According to another aspect of the invention, a method and system is provided that supports multiple currencies.

Elements of an Electronic Commerce Environment. In an electronic commerce payment environment, a requirement is that security and auditing be bound to actual business operations and processes. However, existing methods of public key certificate based authentication and access control disconnects the security infrastructure from the business process. This may be acceptable depending on the scale of the network, but for broad based consumer acceptance, the level of transparency between business and secure technology increases beyond these existing methods. In order to accommodate the demand for a scalable and secure e-commerce environment, a set of elements or conditions are defined and mapped onto the VirtualSAFE invention's secure infrastructure. These elements are based on fundamental security objectives in relation to the entities involved in a typical e-

commerce transaction. These entities include the following: Customer (or User); Merchant / Business; Shipper; Payment Processor; Credit Issuer / Credit Acquirer / Credit Card Vendor; and Bank Account.

In VirtualSAFE, security objectives and business requirements are defined and merged to achieve a cohesive process flow between these entities. These security objectives are based on fundamental principles of confidentiality, entity authentication, data integrity, and non-repudiation. The e-commerce payment protocol of VirtualSAFE, as described herein, provides advantages to the entities involved, as follows:

1. Customer (or User).

    - Customers may affect a confidential purchases from merchants.
    - Only customers may access their purchase data.

2. Merchant / Business.

    - Merchants will have access to the following information: purchase related data submitted by customers; Shipping related data (e.g. personal contact information); and, relevant payment information.

3. Payment Processor.

    - The Payment Processor will require only payment processing credit information.

4. Credit Issuer / Credit Acquirer / Credit Card Vendor.

- The Credit Issuer will require all of the above information.

5. Bank Account.

    - The Bank will require only confirmation of the payment transaction.

The VirtualSAFE invention ensures security through a combination of public key certificates and attribute certificates which are deployed for authentication and authorization purposes for each entity in the typical e-commerce transaction

Referring to FIG. 1, a block diagram illustrating the components **100** of the VirtualSAFE method and system is provided. These components include the following: Public Key Infrastructure (PKI) **101;** Redirection Link **102;** Secure Remote Pointer / Plug-In / Application **103;** Attribute Authority **104;** Virtual Identity **105;** Virtual Smart Card **106;** Secure Data Repository **107;** Authentication Authority **108;** Crypto-Engine (CEV) **109;** Payment Processing Engine **110;** Risk Management Engine **111;** Transaction Fulfillment Mechanism **112;** Insurance Module **113;** Transaction Secure Repository **114;** and VirtualSAFE Deposit Box 115.

These components may be described as follows:

Public-Key Infrastructure (PKI) 101. VirtualSAFE is fully compliant with PKI standards for X.509 v1 and v3 certificates, RSA cryptography, PKCS #11 certificates, S/MIME certificates, PKIX v3 extensions, and Secure Electronic Transactions (SET).

Redirection Link 102. The redirection link allows non-repudiation by using digital certificates and a secure algorithm and protocol residing on a remote merchant or business site.

Secure Remote Pointer/Plug-In/Application 103. A composite secure algorithm and protocol residing on a remote site (VirtualSAFE, merchant, user or any other entity) that provides encrypt/decrypt and digital signing timestamp functionality in communicating with VirtualSAFE.

Attribute Authority 104. An internal and external VirtualSAFE feature that enables the assignment of authorization to users and applications to access network resources and remote non-repudiation providing valid digital signature and verification mechanisms for new or existing financial and other information infrastructures.

Virtual Identity 105. A composite secure algorithm and protocol creating a digital certificate based virtual identity designed on the principle of secret, share secret, and physical material. Current business processes supporting authentication are primarily "shared-secret" based (e.g. PINs, mother's maiden name, SSNs, etc). The "shared-secret" has the disadvantage that the shared-secret can both originate as well as authenticate a transaction (existing business infrastructures need extra levels of security to prevent divulging the shared secret). Upgrading these existing authentication business infrastructures to public key is straightforward and eliminates the vulnerability associated with divulging the authenticating value. Furthermore these are integrated and robust authentication business processes (as compared to the certificate design point for offline email which had no authentication infrastructure). In other words, the existing financial business processes for managing authentication

material can be leveraged for managing public-key authentication material. VirtualSAFE is a straightforward upgrade to all existing shared-secret authentication business processes (upgraded from "shared-secret" to digital signature using existing business processes).

Virtual Smart Card 106. Virtual Smart Card is an internal feature of VirtualSAFE that enables authentication and secure isolated encrypt/decrypt and digital verifying functionality. Remote or roaming VirtualSAFE digital certificate storage is a crucial part of this configuration.

Secure Data Repository 107. An internal VirtualSAFE feature that enables secure storage of dynamic and/or static application data, using a unique PKI based encryption scheme and different crypto-engine security in the same database. Existing standards and business practices allows for VirtualSAFE to maintain an internal secure data repository of certificates in optimized format as long as the original certificate format can be exactly reproduced bit-for-bit. These optimizations are implementation dependent for specific operations and may contain a combination of data compression and/or field elimination.

Authentication Authority 108. An internal and external VirtualSAFE technology that enables the assignment of authorization to users and applications to access network resources and remote non-repudiation providing valid digital signature and verification mechanisms for new or existing financial and other information infrastructures using a multi-tiered authentication authority. The Authentication Authority infrastructure recognizes that in order to validate a digital signature, a certificate containing the corresponding public key must be available. In fact, every

digitally signed object including, but not limited to certificates, which themselves are digitally signed objects requiring additional certificates for validation requires a separate certificate to provide the public key for digital signature validation. This is true for all digitally signed objects and certificates except for the case of a self-signed digital certificate where the public key for validating the certificate's digital signature is included in the body of the certificate.

Crypto-Engine (CEV) 109. See below.

Payment Processing Engine 110. A VirtualSAFE module that enables secure credit or debit card, safe check, wire or any other processing of financial transactions with remote payment providers.

Risk Management Engine 111. A VirtualSAFE component that enables the determination of transaction validity using detailed heuristic processes. Certificate authority digital signatures are not only expensive to manage and computationally burdensome but they place the bank that issues the digital certificates in a position of risk. In a Certification Authority Digital Signature ("CADS") model, the compromise of a CA's private key is catastrophic. Bogus certificates can be issued and fraudulent transactions initiated, all seemingly authorized by the CA. To remedy the situation it would require that the CA re-issue certificates to every certificate holder and to put every previously issued certificate on a CRL. During any time a breach goes undetected, it puts the CA in a position of extreme risk. This systemic risk is why Certification Authorities guard their private keys with expensive physical and procedural security.

The Account Authority Digital Signatures ("AADS") model, on the other hand, carries no systemic risk. Without digital certificates, there is no technical need for a bank to have a private key. Most likely, any bank involved in PKI transactions will likely have a private key, but no certificates (or hierarchy of certificates) are inherently dependent on the security of that key in the AADS model.

As attractive as AADS may sound, it will never eliminate the need for digital certificates. In cases where two parties have no prior relationship, third-party certification makes sense. For example, consider a retail customer wanting to open a new account with a bank over the Internet. The concept of a third-party certificate would aid the bank tremendously in making quick work of the electronic sign-up process. This resembles the role that credit bureaus play today.

Third-party digital certificates will exist. Account authority digital signatures do not preclude the use of CADS. They rely on the same cryptographic operations to validate digital signatures. The latter simply requires additional steps in the validation process. An account authority can easily become a certification authority by applying its digital signature to a customer's public key rather than storing the public key in the account record. If an account authority wants to support trust propagation by issuing certificates, it should, but it should do so based on a conscious business decision. By requiring certificate authority digital signatures, as most existing methodologies do, banks are thrust into the position of propagating trust via digital certificates. It is no longer a business decision but a technical requirement. Banks may not want to take on the risk of trust propagation. As account authorities they don't have to, and they can still remain central to the transaction processing business.

Transaction Fulfilment Mechanism 112. A VirutalSAFE component that completes commercial transactions by means of secure connection with fulfillment providers.

Insurance Module 113. VirutalSAFE provides liability and transaction value insurance. A transaction value insurance algorithm is an active link to the Risk Management Engine. The adjustable architecture of this module provides a full and flexible policy for cumulative, minimum, and contractual coverage related to policy and deductions.

Transaction Secure Repository 114. A VirutalSAFE component that records and securely stores every single transaction that is made by the user.

VirtualSAFE Deposit Box 115. See below.

In the following, an overview of how physical smart cards are currently used and how physical smart card transactions are currently processed is provided. This is followed by a description of how transactions with virtual smart cards are conducted according to the VirtualSAFE invention. A description of a virtual smart card transaction flow according to the VirtualSAFE invention is also provided.

Physical Smart Card Transactions. Typically, local cardholder functions include a consumer card interface. Display and accept/cancel options are performed at the client terminal. Payment functions, including security card control, data storage, and the use of a concentration point, are performed by a payment server. The presentation and eventual delivery of goods and services by a merchant are performed under the

control of a merchant server. The Internet performs routing functions between each entity. It should be appreciated that the Internet may include its present form or it may include any other open network implemented using a combination of computer, telephone, microwave, satellite, or cable networks.

The client terminal controls the interaction with a consumer and interfaces to the card reader that accepts a smart card having a stored-value application. The payment server communicates directly with a terminal or through a concentrator that handles a number of terminals each having a security card. The payment server also communicates with the concentration point for transmission of transaction data to a clearing and settlement system. The database stores all the appropriate information passing through the payment server for each transaction. Use of such a database allows any number of merchants (or merchant servers) to use the payment server for transactions. The payment server controls payment functions such as handling attached terminals, managing the database, and collection functions. The merchant server is typically a site that has contracted with an acquirer to accept smart card transactions as payments for goods and services purchased over the Internet.

As discussed above, the smart card may take a variety of forms and is useful in many situations where it is desirable to store monetary value on a card that a consumer may use. Generally speaking, the smart card is any card or similar device able to store a value and decrement that value when the card is used. The card may be purchased complete with a stored value or a given value may be added to the card later. Such cards may also have their value replenished. The smart card may also perform a variety of functions in addition to simply storing value, for example, debit, credit,

prepayment, and other functions. Such a card typically includes information such as a bank identifier number, a sequence number, a purchase key, a load key, an update key, an expiration date, a transaction ID, and a running balance.

The smart card may include an encryption module in order to provide a variety of security features. For example, security features may include simple PIN numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data Encryption Standard ("DES") or Rivest Shamir Adelman ("RSA") encryption. Typically, a smart card is able to use these features to verify consumers and card readers, to validate security cards, and to provide a unique digital signature. A smart card may include any number of keys which are known to the card issuer and that are used during the course of a payment or load transaction to generate digital signatures for validation of the stored-value card, security card or module, or the system itself.

The client terminal may be any suitable device for interacting with the card and for communicating over a network with a payment server and a merchant server. For example, the client terminal may be a mainframe computer, a workstation, a personal computer, a set top box, a kiosk, or any type of service payment terminal that a consumer might use to purchase goods and services. The client terminal may also be embodied in any portable device including a laptop computer, a cellular telephone (including GSM telephones), or a personal digital assistant ("PDA"). The card reader may be any suitable interface device that is capable of transferring information and commands between the client terminal and the card.

Typically, the client terminal includes a client code module and a card reader module. The reader module may be implemented using any suitable software and libraries for

communicating with the card reader. Its actual implementation will depend upon the type of card reader used. The client module controls communications between the client terminal, the card reader, the payment server, and the merchant server. The client module may be implemented using any suitable software. For example, the client module may be implemented using a combination of "C" code and a Java applet. The applet may be supplemented with parameters from an HTML page sent from the merchant server. The client module is also responsible for controlling displays presented to consumers and for the interaction between the card and the card reader. This module also builds the draw request message after receiving all of the start-up information from the card and the amount of the purchase from the merchant server.

Typically, the payment server includes a payment code module and a terminal interface. As with the client terminal, the payment server may be implemented using any suitable computer, for example, a personal computer. There may be one payment server for each merchant server or a single payment server may service any number of merchant servers. There may be multiple payment servers for a single merchant. In addition, the payment server need not be remote from the merchant server but may be located at the same site and have a different Internet address. Or, the payment server and the merchant server may be implemented on the same computer. The payment server is designed to facilitate communications between the consumer's smart card and a terminal's security card.

The payment module may be implemented using any suitable code. For example, the payment module may be implemented using a combination of "C" code, "C++" code,

and Java code. The payment module may be a multi-threaded process that can service multiple concurrent client applet transactions on demand. The module is responsible for controlling all interactions with terminals including the transaction collection function. For individual transactions, the payment module controls message flow and logs interim results. When an applet connects with the payment server, it creates a transaction thread to support the transaction through its life cycle. Each thread, in turn, assigns a terminal for communications. A one-to-one correspondence between transaction threads and terminals may provide good results.

Typically, the terminal interface is any suitable set of software and libraries for communications with a terminal either directly or through a terminal concentrator. The actual implementation of the terminal interface will depend upon the type of terminal used. For example, an IQ Delta 2010 terminal made by Schlumberger may be used. Such a terminal supports a variety of commands originating from the terminal interface. These commands emulate the normal responses from a smart card to a security card should both be located in the same service payment terminal. The actual security card commands are held in the terminal while the terminal performs the tasks necessary to simulate the presence of a smart card. The emulation of the card commands can be done by the payment server using the terminal as a card reader, or may even be performed by the client terminal.

Typically, the security card is any suitable security card such as those that are known in the art (often referred to as a Purchase Secure Application Module or "PSAM"). The functionality of the security card may be replaced by a crypto-engine (as is done in VirtualSAFE), may be implemented in hardware within the payment server, or may

be implemented in software. For example, the security card may be a removable credit card-sized smart card that is programmed to process and store data relating to financial transactions. The security card may contain a microchip embedded in the card that enables the card to authenticate and to validate the consumer's smart card. If the consumer smart card is acceptable to the security card, and if the smart card contains sufficient value, then the security card guarantees that the merchant providing goods and services will receive payment in the amount deducted from the smart card. The security card may also contains DES and public key purchase security keys, may authenticate the smart card during a purchase transaction, and may secure the payment and collection totals. A security card may also store digital signature algorithms for all smart cards in use. A security card may also contain a transaction identifier for the current transaction, a financial sum of all transactions remaining to be settled, a session key, and master keys for all smart cards in use. Further, the security card may contain generations of keys, blocked card indicators, dates of last update, multiple card programs, different currency rates, and additional security.

The concentration point is typically a staging computer that communicates with a payment server to collect batches of purchase transactions. The concentration point then sends these transaction batches to a clearing and settlement system for processing. Once processed, batch acknowledgments, along with other system updates, are returned.

Typically, the merchant server includes a merchant code module. The merchant server may be implemented on any suitable computer capable of communicating with and presenting information to consumers over the Internet. The merchant code module

may be implemented using any suitable code. For example, the merchant module may be implemented using a combination of Perl, HTML, and Java code. The merchant server is typically a generic web server customized for the merchant's business. The merchant server may include databases, CGI scripts, and back-office programs that produce HTML pages for an Internet user.

Physical Smart Card Transaction Flow. During a financial transaction, the client terminal and the merchant server exchange information via the Internet. Each transaction initiated by a consumer has a transaction identifier created at the merchant server. A merchant identifier unique to the payment server is also available from the merchant server. The client module and the payment server also use this unique transaction identifier for tracking and logging information about the transaction. The merchant server generates a unique identification for the transaction, completes other required parameters, encrypts as appropriate, and builds an HTML page and sends it to the client terminal. The client code module interacts with the smart card and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server.

Next, the client terminal communicates with the payment server by first forwarding the draw request to the payment server. The payment server verifies the transaction to determine if it is a valid transaction from a known merchant. The transaction is logged in the payment server's transaction database. Upon completion of a transaction, the payment server builds a result message containing the identification of the transaction and signs it. The message is then routed to the merchant server via the client terminal. The merchant server then validates the result message. After determining that the

transaction was successful, the merchant server creates an HTML page for the purchased information and sends it to the client terminal. The merchant may also deliver purchased goods and services to the consumer at this point. It is also possible for the payment server and the merchant server to communicate information directly between them. As the client terminal has already established communication with the merchant server and the payment server, links are used to exchange information between the payment server and the merchant server, rather than establishing a new link.

Transactions With Virtual Smart Cards. Similar to transactions with physical smart cards, this system includes the client terminal, the payment server, and the merchant server. However, the system dispenses with the need for the card reader and the physical smart card as their functionality is contained within the online purchase and initiation server (i.e. VSAA). The client code module is now functionally part of the VSAA server instead of being part of the client terminal. And, the functionality of the card reader module for transactions with physical smart cards is now included within the client code module to allow communication with the pseudo technology process module. Also, the user interface functionality of the client code module is transferred to a client terminal module of the client terminal. In this embodiment, the pass-through client module serves to "pass through" communications between the merchant server and VSAA server.

The VSAA server effectively replaces the need for a physical smart card and physical card reader within the system. To achieve this goal, the VSAA server implements a "pseudo technology process module" and the smart card emulator in software. A card

database stores information representing "virtual" smart cards in use within the system. The card emulator interacts with the card database and a the VirtualSAFE crypto-engine ("CEV") to effectively replace the physical smart card and reader. Thus, the client code module may be implemented as before unaware that it is interacting with a software emulation of a smart card rather then with a physical smart card.

The VSAA server stores the same data used with physical cards in its database and handles incoming commands from initiation or payment servers to increment or decrement a "card" balance as appropriate. Important data is stored in encrypted form and all functions that require a change to important data or the generation or checking of digital signatures is performed in the CEV. The VSAA server resides at an issuer's site or at its designated processor. One such server may support multiple issuers provided appropriate safeguards are in place to partition that data.

Furthermore, to support interoperability with present financial networks, including different credit card vendors, financial institutions, and processing gateways, the VSAA server may reside at the acquirer's site or at any processor. This setup does not change the present flow and does not require additional investment to secure the financial network.

In an alternative embodiment, the client terminal also includes a card reader and a smart card. For this embodiment, included in the client terminal is a client code module, in addition, to pass through the client module. In this alternative embodiment, the system may operate in either of two modes. The system may operate without using a physical smart card by using the emulation contained within the

VSAA server. Concurrently, or at a later date when smart cards and readers are more common, the system may be upgraded to make use of a physical card and reader attached to the client terminal.

The VSAA server communicates with the client terminal through a user verification module and with the payment server over a link. The VSAA server emulates a physical smart card through the use of the pseudo technology process module, a smart card emulator, a crypto-engine (CEV), and the card database.

The financial information database and secure data repository is a database implemented in any suitable format and contains a record of information for each virtual smart card in use within the system. The financial information database and secure data repository includes the information for each virtual smart card in use and thus helps to simulate a physical smart card. An identifier such as a user name, PIN, or some combination is used as an index into the database in order to identify the appropriate virtual card for initiating, debiting, or authentication. Also, it is preferable that the information contained in the database is stored in an encrypted form for security. In one embodiment, the database is implemented in Sybase.

Records in the database store a variety of data for each virtual smart card. This information includes initiation and purchase key identifiers, card and issuer certificates, initiation algorithms, initiation key versions, purchase algorithms, purchase key versions, a bank identification number (BIN), a VirtualSAFE Deposit Box ("VSDB") number, a transaction ID, a balance, a currency and exponent, an expiration date, and a maximum balance.

Initiation and business public keys indicate which keys should be used. Although all keys may be stored within CEV, in one embodiment, the keys are stored within the database as well, with the exception of the CEV master key that is stored in the CEV.

Initiation algorithms are identifiers that identify which cryptographic algorithm of the CEV is to be used for the verification and generation of digital signatures during an initiation. The initiation key version is an identifier identifying which version of a key will be used for the generation or verification of a particular digital signature. Purchase algorithms and purchase key versions perform a similar function during a purchase.

A six-digit BIN in combination with the ten-digit TEP forms a sixteen-digit identification number that uniquely identifies a particular virtual smart card. This identification number is also known as a VSAA card identifier. Each BIN, or card range, has a single maximum balance and currency for all of its virtual cards. The balance keeps track of the value for the particular card. Currency and exponent information provide further details concerning the balance.

Expiration date provides an expiration date for the card. The maximum balance provides a maximum for the virtual card, or could also indicate a maximum balance for all virtual cards associated with a BIN.

The VirtualSAFE crypto-engine (CEV) is used to facilitate cryptographic processing. The CEV stores secret keys and encryption algorithms, performs cryptographic functions on secret data and generates digital signatures. As is known in the art, the CEV is generally a tamper-proof device that uses some level of physical security

means to protect the sensitive information inside. CEV may be any security module used in the industry, or similar to the security box attached to automatic teller machines. In alternative embodiments, the CEV may be implemented on a smart card within a card reader, on a series of smart cards, on any suitably secure computer, or in software.

The CEV performs the role of an encryption module for a physical smart card in addition to other tasks. For a physical smart card, various data elements such as balance and currency are contained securely within the smart card. However, such data elements are not stored within the CEV but are stored on the server in the card database. For such important information, these data elements are stored in an encrypted form in the database. Thus, the CEV performs the additional task of receiving encrypted card data from the database via an emulator, decrypting the card data, performing any cryptographic functions upon the data, and then encrypting the data and sending it back out to be stored in the financial information database and secure data repository. For example, if the card balance is to be reduced, the encrypted balance is sent from the database to the CEV where it is decrypted, reduced, and then finally encrypted again before it is returned to the database.

The CEV also performs cryptograph functions related to digital signatures used within the system. Digital signatures are used during the initiation operation and typically are generated by the smart card. Some digital signatures are used during an initiation or purchase operation and are generated by the issuer or the payment server. Some digital signatures are generated by the smart card on occurrence of an initiation or debit and are considered the final digital signature after the card has either initiated

value onto, or debited value from, itself. In the VirtualSAFE invention, the CEV performs these functions that are normally handled by a smart card because no physical smart card is present. The CEV is used to generate digital signatures and verify digital signatures for an initiation operation, and is used to verify digital signatures and generate digital signatures for a purchase operation. The CEV may also perform other cryptographic functions that would normally be performed by a physical smart card.

The transaction database stores information regarding transactions that occur such as a debit or an initiation and may be implemented in a similar fashion as the database. Also known as a history database, the database includes a purchase table (i.e. log full of transactions and timestamps) and an initiation table (i.e. log full of transactions, funding request/response, and timestamps).

The pseudo technology process module is a software module that performs the functionality of a physical card reader so that the emulation of a smart card is transparent to the client code module. The card reader module accepts the actual card reader commands from the client code module and, instead of using them to drive a physical card reader, places them into a format to communicate with the smart card emulator that is emulating a smart card. Thus, an existing application programming interface (API) used by the client code module to communicate with a smart card may continue to be used. In an alternative embodiment, the card reader module and the emulator may be collapsed into a single functional block although this may require modification of the commands issued by the client code module.

The user verification module allows the VSAA server to identify which user is logged on to the system and desires access to a virtual card in the card database. The module provides a login procedure that requires a secret user identifier and PIN from each user. A combination of this user identifier and PIN is then used as an index into the card database to identify the record that represents the virtual smart card for that user. The user verification module may also include the VSAA card identifier (digital certificate digital signature) for the user, the funding account and its expiration date, and address information for address verification during the funding portion of the initiation transaction. An address verification system may compare billing information from an authorization to that on file to assure that the real cardholder is making the transaction.

The smart card emulator emulates a physical smart card by accepting and passing the incoming card commands from the card reader module and determining actions to perform. In the course of performing these actions, the emulator handles the interface to the CEV, fetches data from, and stores data to, the card database. For example, upon receiving a command to debit a card, the emulator fetches the balance from the appropriate record in the database and transfers the encrypted balance to the CEV to be decrypted and decremented. Once the new balance is encrypted by the CEV, the emulator receives the new balance and stores it back in the transaction secure database.

Once an action has been performed, the VirtualSAFE process technology emulator generates a simulated smart card response that is then relayed via the card reader module and the client code module to the payment server. The VirtualSAFE process

technology emulator generates card commands that appear as if they have been generated by a physical smart card, thus making emulation of the smart card transparent to the rest of the system. The emulator also updates the transaction database at appropriate steps in the processing of a debit or an initiation.

In addition to debiting or initiating a virtual card in the card database, the VSAA server is able to credit a virtual card if the card was debited by mistake. In other words, once a card has been debited to make a payment, the VSAA server is able to recover that value and credit the virtual card in the card database, if necessary. For example, if a transaction fails and value has been taken off the card, but no value has been credited to a particular payment server, the system is able to credit the virtual card in the card database to replace the lost value. Such an operation is different from a formal initiation command in that a user's card is credited for a value that had earlier been taken off the card.

Virtual Smart Card Transaction Flow. One embodiment of an Internet payment and initiating system includes the client terminal, the payment server, the merchant server, and the online purchase and initiation (VSAA) server. A virtual smart card inside the terminal is in communication with the payment server and other modules supported by a multi-tiered authentication authority.

One method by which a financial transaction may be completed over the Internet using a virtual smart card will now be described.

Initially, a suitable web browser initiated on the client terminal is used to access a merchant server web site. The user selects goods and/or services from the merchant

site and indicates to the site that the he or she wishes to purchase these items using a virtual smart card.

The merchant server receives this request for a virtual card transaction.

The merchant server builds an HTML page that includes several parameters. These parameters include the total cost of the transaction as determined by the merchant server, the type of currency being used, the port and IP address of the payment server, and a unique transaction identifier used by both the payment server and the merchant server to track a transaction. Also included is a unique merchant identifier assigned to the merchant by the acquirer and known to the payment server. Other information may also be included such as the currency's exponent, a status URL address of the merchant server used for communication from the client terminal, and a merchant server generated key and other security information to ensure the identity of the merchant server and the integrity of the message. Other process related information such as software release level, encryption methodology, and keys may also be conveyed. Once this page has been built, the page is sent to the requesting client browser and triggers the initiation of a client terminal module in the client terminal.

Some browsers may not allow an applet to invoke a dynamic link library ("DLL") due to security reasons. As such, in one embodiment of the invention, the client terminal applet, along with any DLLs needed, are pre-initiated on the client terminal. Then, the merchant server is allowed to invoke the client terminal applet and DLLs dynamically to circumvent this security precaution. In an alternative embodiment, the client applet is signed to ensure its authenticity and integrity.

The client terminal module then displays a screen containing the amount provided by the merchant and requests that the user authorize the amount by entering their user identifier (which preferably is masked on screen) and PIN. Once entered, the client terminal module routes the purchase request (including purchase parameters from the merchant server, user identifier and PIN) to the VSAA server. The VSAA server then validates the user identifier and PIN with the user verification module.

The client code module of the VSAA server then interacts with the pseudo technology process module to build a draw request message for later transmission to the payment server. It should be noted that at this point two types of emulation occur. The VSAA server neither includes a physical smart card nor a virtual smart card. The physical card is represented as a virtual card in a record of the card database, while the virtual smart card is attached to a remote payment server. Thus, the client code module will emulate commands that a virtual smart card would issue to build the draw request, while the pseudo technology process module, the smart card emulator and the database emulate a physical smart card.

In one embodiment of the invention, the client code module initiates a local DLL, makes an API call to that library, which in turn makes a call to another DLL that finally makes a call to the pseudo technology process. An "Initiate VSDB for Purchase" command (Initiate VSDB) is created and forwarded to the emulator via the card reader module. This command is modified in a suitable fashion to identify which record in the database will be debited (i.e. which virtual card). For example, the user identifier or PIN may be included. Next, the emulator parses the incoming command and does a database fetch to obtain the virtual card record from the database. In

another embodiment of the invention, the fetch may be optimized to only retrieve certain information. The emulator then sends the record to the CEV for decryption of the card data found in the record.

Once responses to the "Initiate IE-W" (i.e., intersector electronic wallet) command from the reader are received, the client module combines these responses into a byte stream suitable for transmission over a network to a payment server. Also at this point, the currency type and expiration date of the virtual card in the database are checked, and the total cost of the ordered merchandise is checked against the card balance to ensure that the value on the card is great enough to cover the transaction. If the checks are not successful, a message to that effect is delivered to the user and the transaction terminates.

Since the virtual smart card is remotely located, it would not be advantageous to engage in numerous commands and responses between the virtual smart card and the client code module over an open network such as the Internet. In the interests of speed and reliability, it is advantageous to have fewer messages exchanged. Accordingly, the client module emulates a variety of virtual smart card commands in order to receive responses to these commands from the pseudo technology process. To operate securely and reliably in this environment, in one embodiment of the present invention, the client module emulates a virtual smart card and gathers all the responses for transmission in one draw request message. The commands and responses take place between the client code module and the pseudo technology process as if there were an actual card reader with a physical smart card inside. In other words, the client code module need not be aware that a virtual card is being

used. The draw request message may include a variety of data including a draw request token, state information, the merchant identifier, the transaction identifier, security information, a wallet provider identifier, and an intersector electronic wallet ("IE-W") identifier. Also the message may include an algorithm used by the card, an expiry date, the balance of the card, a currency code, a currency exponent, the authentication mode of the IE-W, the transaction number of the IE-W, a key version, and the purchase amount. As all of this information is prepackaged into a single draw request message, the number of messages over the Internet between the VSAA server and the payment server is greatly reduced.

In one embodiment, the draw request message is built by packaging the virtual card's response to the "Reset" and "Initiate IE-W for Purchase" commands, any public key certificates, the total cost, and the currency of the transaction received from the HTML page. For public key cards, the card and the issuer certificates are obtained from read commands and may also be included in the draw request. By packaging all of this information together into one draw request message, it is possible to cut down on the number of messages exchanged between the VSAA server and the payment server and hence reliability and speed are improved.

Next, the VSAA server accesses the payment server using the IP address received from the merchant server. The VSAA server sends the draw request message to the payment server. The VSAA server also creates a log of the message being sent.

The payment server sends to the client terminal the draw request and processes the draw request in conjunction with an associated virtual smart card. In one embodiment of the invention, the payment server creates a transaction thread for each connected

client module to service it through the life cycle of the transaction. The payment server receives a debit command and a virtual smart card digital signature from the virtual smart card.

The virtual smart card digital signature is a value that uniquely identifies and validates the virtual smart card to prove to the VSAA server that the incoming debit command is a valid command from a real virtual smart card. This validation ensures that when the virtual card is debited the financial totals in the virtual smart card are updated. Thus, the user of the virtual card is guaranteed that a valid debit of the card has occurred. In one embodiment of the invention, the virtual smart card digital signature is an encrypted value ensuring that no other entity can forge an identity of a virtual smart card.

The payment server sends the debit command along with the virtual smart card digital signature to the VSAA server to allow the virtual card to accept the debit. At this time, the payment server also logs the debit command into its database. Upon receiving the debit command from the payment server, the client module replaces the amount in the debit command with the original amount (from the merchant server) to ensure that the amount has not been tampered with while traveling over the network. At this time, the client module may also create a log of the debit command.

The client module forwards the debit command and virtual smart card digital signature to the emulator and it again retrieves the appropriate virtual card record from the database for processing. The card record is retained in memory while a transaction is occurring. The card record, debit command, and digital signature are sent to the CEV where the virtual smart card digital signature is verified and a virtual

card digital signature is generated. The card record is updated in the CEV with revised parameters (including balance and transaction ID) to reflect the purchase transaction and returned to the card database. The client module receives the CEV response and generates a "Debit Response" message along with the card digital signature. If the virtual card does not have enough value to satisfy the purchase amount, then a "Debit Response" message indicates as such. The card digital signature is a unique value identifying a valid virtual card in the card database. In one embodiment of the invention, the digital signature is in encrypted form to prevent tampering.

The emulator sends the response message along with the card digital signature back to the client module. At this point, the purchase amount has been deducted from the balance on the virtual card (assuming a successful transaction). Next, the client module packages the response message along with the card digital signature and sends them back to the payment server. The client module also logs the result of this virtual card debit.

The payment server receives the incoming message and creates a log and updates the transaction status in its database for future error recovery. The payment server then directs this received message to the virtual smart card in the terminal. Next, the virtual smart card processes this response from the VSAA server and verifies the received virtual card digital signature.

As the virtual smart card contains the keys and algorithms necessary to compute card digital signatures, the virtual smart card is able to validate that a received virtual card digital signature is in fact a valid one by comparing this card digital signature with a

generated expected value. A successful comparison indicates that a response message received from the virtual card is in fact a valid message and that the virtual card has been debited. An error result code or a comparison that is not successful potentially indicates that the virtual card has not been debited. This comparison of card digital signatures by the virtual smart card ensures that a virtual card is in fact debited before the merchant server is directed to release the purchased merchandise to the user. The virtual card digital signature is compared to an expected value and performed by the virtual smart card for the highest level of security possible. This comparison of virtual card digital signatures may also take place in the payment server, in the VSAA server, in the client terminal, or in the merchant server, with a variety of other advantages. Assuming that the transaction is so far valid, the virtual smart card sends a response indicating the result of the digital signature verification. The payment server uses this response to build a "Debit Result" message. If the transaction was invalid or if the verification failed, then an exception would be returned.

The terminal updates its data store with the virtual card number, a transaction count, and the total sale amount. Also updated is the response from the virtual smart card and transaction numbers from the virtual card and from the virtual smart card. The payment server also logs the response received from the terminal along with the merchant identifier, etc. Next, the payment server packages the result message including the transaction identifiers and sends this message to the VSAA server in encrypted form. The server then passes the result to the emulator for appropriate database updates such as balance and ID. The transaction is also logged in the history file.

The result message is then forwarded to the client terminal. At this point, the transaction thread of the payment server that was used for the current transaction may release the terminal, thus allowing the terminal to be used by other transactions. The transaction thread then exits at this time.

By sending this result message in encrypted form, the confirmation included in the message may be passed to the merchant server by way of the client terminal without fear of tampering. As the result message is encrypted, it would be extremely difficult for the client terminal or another entity to forge a confirmation and trick the merchant server into thinking that a transaction had taken place. In one embodiment of the invention, if the client terminal is a trusted agent, then the result message need not be encrypted. In yet another embodiment of the invention, the payment server may send two confirmation messages, one not encrypted for the client terminal to process, and one encrypted for the merchant server, or both messages encrypted under different keys.

The client terminal then passes the result message on to the merchant server at the URL address previously received from the merchant server. The client may also post a message to the user informing that the debit has been completed. The client may also log confirmation of the payment. The merchant server registers the confirmation included in the message and checks for success. The merchant server calls a validate routine within the merchant code module to validate the result message received via the client terminal. The validation routine decrypts the transaction identifier along with the encrypted result message. If the decrypted result message is acceptable, the merchant server then determines that a successful transaction has occurred. Next, the

merchant server generates a message with the purchased information and delivers this information to the client terminal. The merchant server may generate a purchase receipt to deliver to the client terminal indicating that goods and services are to be rendered. At this point, the client terminal may log the merchant server's response. Completion of these steps indicates a successful financial transaction over the Internet using a virtual smart card.

For greater clarity, a description of the invention from a user's perspective is provided as follows.

The VirtualSAFE Invention From A User's Perspective. A user sets up his or her virtual card within the system. In one embodiment of the invention, a physical card in the possession of the user is used to provide some of the information requested by the VSAA server. The user accesses the VSAA server over the Internet using a VSAA login URL to access the user verification module. A screen is presented to the user which requests that the user enter his or her user identifier, a funding account number, the card verification value ("CVV"), expiration date of that account, billing address, electronic mail address, and a chosen PIN. (The card verification value is a 3-digit value on the digital signature panel of a card and is used internationally for fraud deterrence.) The first time the user identifier is entered it is in the clear. However, when the identifier is entered again by the user, this time perhaps for a transaction, it appears masked on the screen so as to be kept secret. The user verification module

then presents a screen to the user indicating that a confirmation will be sent to the user's electronic mail address. The user then logs out.

Later, an electronic mail confirmation is sent that contains a one-time logon PIN. The user receives the electronic mail and begins the setup process by logging on to the URL of the VSAA server and entering his or her user identifier and one-time PIN for checking by the user verification module. Once these are verified, the user is prompted to change the one-time PIN to a new user-selected PIN. The user verification module then assigns a unique identification number ("VSAA card identifier") to the user.

During this session or at a later time, the user initiates value onto the virtual card. Initiation may be accomplished in several different ways. In one embodiment of the invention, a virtual card may come pre-initiated with a certain amount when an account is set up, that is, the balance in the database is positive for a particular record. Other methods of initiation may also be used.

The user accesses the merchant server web site via a communication link over the Internet. This web sit access may be performed in any suitable fashion such as by using any commercially available web browser. Once at the merchant web site, the user is prompted to choose payment via either a physical smart card or via the virtual smart card of the present invention. If the user chooses payment via a physical smart card, then a purchase may proceed as described in U.S. Patent Application No. 08/951,614, which is incorporated herein by reference. If the user chooses the virtual card method, then the user is prompted for his or her user identifier (which preferably is masked on screen) and PIN that is verified by the VSAA server.

Next, the user browses the merchant web site and selects goods and services for purchase from the merchant using the web site interface that the merchant has provided. The user then selects an appropriate button on the merchant web site to indicate what the user wishes to make a purchase. Next, the user receives a total sale amount from the merchant server, a current balance from the VSAA server, and is directed to actuate a button on the web site indicating that the user wishes to proceed with the purchase using the virtual card.

The system processes the user order by way of the payment server, the VSAA server, the terminal, and the virtual smart card. The user's virtual smart card is debited by the total sale amount and the user receives a "debited" message at the user's terminal. This message is optional and is dependent on system design. The user receives a confirmation message from the merchant server indicating that the transaction has been completed. The user may now download the purchased information and/or receive a receipt for goods and services to be rendered or delivered from the merchant at a later date. The merchant, via a clearing and settlement system, receives payment to its bank account for the goods and services rendered by way of information collected from the payment server. In one embodiment of the invention, an existing clearing and settlement system is used as is existing methodology for transferring information from a smart card for later reconciliation. This use of an existing "back end" allows the present invention to be implemented more quickly and less expensively.

Referring to FIGURES 3 through 12, the method of enrolling new users and CA processes in the VirtualSAFE invention are described in detail in the following.

Enrolment Procedure. The following is a description of the enrolment and sign-up process when a user is initially introduced and registered as a primary new user within VirtualSAFE.

Merchant Enrolment. For Merchant enrolment, the Merchant has to authenticate an authorized person for VirtualSAFE. Afterwards, that person enrolls the business filling in the required information and sending by e-mail or e-fax a copy of the required information and documents for necessary credit checks by a credit bureau or equivalent as per local government regulations. VirtualSAFE is completely flexible and supports international organizations.

User Enrolment: Case 1. FIG. 3 is a flowchart indicating the steps for user enrollment in VirtualSAFE in the general case.

User Enrolment: Case 2. FIG. 4 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: No Web certificate + Full VirtualSAFE Sign-Up Process + Payment Processing. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the User's WEB Certificate present?

The system checks to see whether or not the User's WEB certificate is present. In the case illustrated by FIG. 4, it isn't available or present. Therefore, message 407.3 gets sent through VirtualSAFE Web Certificate present site to the VirtualSAFE Web Certificate not present site indicating that no Web Certificate exists to authenticate the user.User redirected.

Step 4 – No Certificate SSL Session

SSL session is established by the Web Server generated a temporary user session certificate.

Step 5 – Existing VirtualSAFE User

Is the user an existing VirtualSAFE client or is this the first time they are trying to sign-up and process a payment? NO

Step 6 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 7 – Enrolment/registration page

The client is hyperlinked to the Enrolment/registration page where they enter their personal data, credit data, email data, etc. Note: The data entered by the user will never ever have to be entered again, as all of the information provided will be stored in VirtualSAFE. Once the user has completed entering their information:

Step 8 – Partial Enrolment

- A VirtualSAFE certificate will be created for the user
- The user's data and the user's VirtualSAFE certificate will be stored to the Secure Data Repository.
- All of the user's VirtualSAFE data will be stored to the VirtualSAFE x500
- The user's WEB certificate will be created
- The user's WEB certificate will be downloaded and sent to them
- The user's WEB data will be stored to the WEB x500

Step 9 – Confirmation to the user – Full enrolment

Would you like to enroll with VirtualSAFE? YES

Step 10 – Enrolment to VirtualSAFE community

This is where the final user setup is confirmed and additional data is encrypted with the VirtualSAFE Certification Authority Public Key, which also includes:

- 1st identification string
- 2nd identification string
- Dynamic PIN (pre-generated number)
- Additional data encrypted with a VirtualSAFE CA Public Key
- And, any keyword(s) that may be need for further authentication

Step 11 – The enabler

The user has become a registered and authenticated VirtualSAFE user and can now shop anywhere on the net, their information is stored in encrypted form to Oracle, or any database, etc., and an email of registered confirmation is sent to them, as well as a cancellation procedure.

User Enrolment: Case 3. FIG. 5 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: No WEB certificate + Only Payment Processing . The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the User's WEB Certificate present?

The system checks to see whether or not the User's WEB certificate is present. In the FIG. 5 case, it isn't available or present. Therefore, message 407.3 gets sent through VirtualSAFE Web Certificate present site to the VirtualSAFE Web Certificate not present site indicating that no Web Certificate exists to authenticate the user. User redirected.

Step 4 – No Certificate SSL Session

SSL session is established by the Web Server generated a temporary user session certificate.

Step 5 – Existing VirtualSAFE User

Is the user an existing VirtualSAFE client or is this the first time they are trying to sign-up and process a payment? NO

Step 6 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 7 – Enrolment/registration page

The client is hyperlinked to the Enrolment/registration page where they enter their personal data, credit data, email data, etc. Note: The data entered by the user will never ever have to be entered again, as all of the information provided will be stored in the VirtualSAFE. Once the user has completed entering their information:

Step 8 – Partial Enrolment

- A VirtualSAFE certificate will be created for the user
- The user's data and the user's VirtualSAFE certificate will be stored to the Secure Data Repository.
- All of the user's VirtualSAFE data will be stored to the VirtualSAFE x500
- The user's WEB certificate will be created
- The user's WEB certificate will be downloaded and sent to them
- The user's WEB data will be stored to the WEB x500

Step 9 – Confirmation to the user – Full enrolment

Would you like to enroll with VirtualSAFE? NO

Step 10 – The enabler

The user has become a registered and authenticated VirtualSAFE user and can now shop anywhere on the net, their information is stored in encrypted form to Oracle, our any database, etc., and an email of registered confirmation is sent to them, as well as a cancellation procedure.

User Enrolment: Case 4. FIG. 6 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: No Web certificate + Already a VirtualSAFE member + Known PIN. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the User's WEB Certificate present?

The system checks to see whether or not the User's WEB certificate is present. In the FIG. 6 case, it isn't available or present. Therefore, message 407.3 gets sent through VirtualSAFE Web Certificate present site to the VirtualSAFE Web Certificate not present site indicating that no Web Certificate exists to authenticate the user. User redirected.

Step 4 – No Certificate SSL Session

SSL session is established by the Web Server generated a temporary user session certificate.

Step 5 – Existing VirtualSAFE User

Is the user an existing VirtualSAFE client or is this the first time they are trying to sign-up and process a payment? YES

Step 6 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 7 – Identification strings authenticated

- 1st identification string
- 2nd identification string
- Search of x500 directory is done

Step 8 – Is the user authenticated?

The system checks the VirtualSAFE x500 for verification.YES.

Step 9 – Creates new WEB certificate

Once the user has been authenticated, the system creates a new WEB certificate and downinitiations it to the client, and the Session Cookie is sent to the user.

Step 10 – PIN identification (policy)

The system displays to the user the PIN Identification Policy page.

Step 11 – Encrypted PIN authentication page

The system checks to ensure whether the encrypted PIN number entered by the user matches the encrypted PIN on the system.

If YES, the encrypted PIN matches, then the user is sent to: Step 12 - User Preference Page, and then to wherever they would like to shop on the net.

However, if NO the encrypted PIN doesn't match, then the method of FIG. 5 is followed.

User Enrolment: Case 5. FIG. 7 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: No Web certificate + Already a VirtualSAFE member + Unknown encrypted PIN + email notification. The following steps are included:

Step 1 – PIN authentication page

The system checks to ensure whether the encrypted PIN number entered by the user matches the encrypted PIN on the system. If NO the encrypted PIN doesn't match, then: Message is sent by email to the user, and the user is redirected to the WEB enrolment page.

Step 2 – Enrolment/Registration page

The client is hyperlinked to the Enrolment/Registration page where they re-enter/or confirm their personal data, credit data, email data, etc. Note: The data entered by the user will never ever have to be entered again, as all of the information provided will be stored in the VirtualSAFE. Once the user has completed entering their information:

Step 3

- A VirtualSAFE certificate will be created for the user
- The user's data and the user's VirtualSAFE certificate will be stored to the Secure Data Repository.
- All of the user's VirtualSAFE data will be stored to the VirtualSAFE x500
- The user's WEB certificate will be created
- The user's WEB certificate will be downinitiationed and sent to them
- The user's WEB data will be stored to the WEB x500

Step 4 – Confirmation to the user

Would you like to enroll with VirtualSAFE? NO

Step 5 – The enabler

The user has become a registered and authenticated VirtualSAFE user and can now shop anywhere on the net, their information is stored in encrypted form to Oracle, our any database, etc., and an email of registered confirmation is sent to them, as well as a cancellation procedure.

User Enrolment: Case 6. FIG. 8 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: No Web certificate + Already a VirtualSAFE member + no x500 entry. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the User's WEB Certificate present?

The system checks to see whether or not the User's WEB certificate is present. In the FIG. 8 case, it isn't available or present. Therefore, message 407.3 gets sent through VirtualSAFE Web Certificate present site to the VirtualSAFE Web Certificate not present site indicating that no Web Certificate exists to authenticate the user. User redirected.

Step 4 – No Certificate SSL Session

SSL session is established by the Web Server generated a temporary user session certificate.

Step 5 – Existing VirtualSAFE User

Is the user an existing VirtualSAFE client or is this the first time they are trying to sign-up and process a payment? NO

Step 6 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 7 – Identification strings authenticated

- 1st identification string
- 2nd identification string
- Search of x500 directory is done

Step 8 – Is the user authenticated?

The system checks the VirtualSAFE x500 for verification. NO.

Step 9 – Enrolment/Registration page

The client is hyperlinked to the Enrolment/Registration page where they re-enter/or confirm their personal data, credit data, email data, etc.

Note: The data entered by the user will never ever have to be entered again, as all of the information provided will be stored in the VirtualSAFE. Once the user has completed entering their information:

Step 10

- A VirtualSAFE certificate will be created for the user
- The user's data and the user's VirtualSAFE certificate will be stored to the Secure Data Repository.
- All of the user's VirtualSAFE data will be stored to the VirtualSAFE x500
- The user's WEB certificate will be created
- The user's WEB certificate will be downinitiationed and sent to them
- The user's WEB data will be stored to the WEB x500

Step 11 – Confirmation to the user

Would you like to enroll with VirtualSAFE? YES/NO

Step 12 – The enabler

The user has become a registered and authenticated VirtualSAFE user and can now shop anywhere on the net, their information is stored in encrypted form to Oracle, our any database, etc., and an email of registered confirmation is sent to them, as well as a cancellation procedure.

User Enrolment: Case 7. FIG. 9 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: Web certificate + Unknown/Known PIN. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the WEB Certificate present?

The system checks to see whether or not a WEB certificate is present. In the FIG. 9 case, the WEB certificate is present.

Step 4 – WEB Certificate is present

The system performs a two-way authentication process.

Step 5 – Checks VirtualSAFE certificate - x500

The system checks the VirtualSAFE x500 to Electronically Authenticate the computer.

Step 6 – Checks for VirtualSAFE certificate

The system checks for a VirtualSAFE certificate by flagging the VirtualSAFE x500 directory. When the system confirms that the VirtualSAFE certificate is available, the user is routed to Step 7.

Step 7 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 8 – Identification strings authenticated

- 1st identification string
- 2nd identification string (optional)
- Search of x500 directory is done

Step 9 – Is the user authenticated?

The system checks the VirtualSAFE x500 for verification. YES.

Step 10 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 11 – PIN identification (policy)

The system displays to the user the PIN Identification Policy page.

Step 12 – PIN authentication page

The system checks to ensure whether the PIN number entered by the user matches the PIN on the system. If YES, the PIN matches, then the user is sent to: Step 13 - User Preference Page, and then to wherever they would like to shop on the net. However, if NO the PIN doesn't match, then the FIG. 7 method is followed to completion.

User Enrolment: Case 8. FIG. 10 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: Web certificate (No VirtualSAFE) + Unknown/Known PIN. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the WEB Certificate present?

The system checks to see whether or not a WEB certificate is present. In the FIG. 10 case, the WEB certificate is present.

Step 4 – WEB Certificate is present

The system performs a two-way authentication process.

Step 5 – Checks VirtualSAFE x500

The system checks the VirtualSAFE x500 to Electronically Authenticate the user. The e-authenticate interoperable module checks the validity of the web certificate by checking the content of the directory of the originating CA. The VirtualSAFE Policy will determine whether the VirtualSAFE directory, or the originating directory is checked or both are checked.

Step 6 – Checks for VirtualSAFE certificate

The system checks for a VirtualSAFE certificate by flagging the VirtualSAFE x500 directory. If the VirtualSAFE certificate cannot be verified, then the user will go to Login to VirtualSAFE/Enrol in VirtualSAFE to be confirmed and then carry on to Step 7.

Step 7 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 8 – Identification strings authenticated

- 1st identification string
- 2nd identification string (optional)
- Search of x500 directory is done

Step 9 – Is the user authenticated?

The system checks the VirtualSAFE x500 for verification. YES.

Step 10 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 11 – PIN identification (policy)

The system displays to the user the PIN Identification Policy page.

Step 12 – PIN authentication page

The system checks to ensure whether the PIN number entered by the user matches the PIN on the system. If YES, the PIN matches, then the user is sent to: Step 13 - User Preference Page, and then to wherever

they would like to shop on the net. However, if NO the PIN doesn't match, then the method of FIG. 5 is followed to completion.

User Enrolment: Case 9. FIG. 11 is a flowchart indicating the steps for user (or resource) enrollment in VirtualSAFE in the following case: WEB certificate (No VirtualSAFE) + Enrolment/Payment Process. The following steps are included:

Step 1 - ACCESS

User decides the proceed with purchase (BUY)

Step 2 – SSL Certificate Handshake Attempted

The first authentication takes place as soon as the User has been accepted as a Registered User Site by use of the Secure Sockets Layer (SSL).

Step 3 – Is the WEB Certificate present?

The system checks to see whether or not a WEB certificate is present. In the FIG. 11 case, the WEB certificate is present.

Step 4 – WEB Certificate is present

The system performs a two-way authentication process.

Step 5 – Checks VirtualSAFE x500

The system checks the VirtualSAFE x500 to Electronically Authenticate the user. The e-authenticate interoperable module checks the validity of the web certificate by checking the content of the directory of the originating CA. The VirtualSAFE Policy will determine whether the VirtualSAFE directory, or the originating directory is checked or both are checked.

Step 6 – Checks for VirtualSAFE certificate

The system checks for a VirtualSAFE certificate by flagging the VirtualSAFE x500 directory. When the system confirms that the VirtualSAFE certificate is available, the user is routed to Step 7. If the VirtualSAFE certificate cannot be verified, then the user will go to Login to VirtualSAFE/Enroll in VirtualSAFE to be confirmed and then carry on to Step 7.

Step 7 – Active X/Java Applet/Application sends dedicated public WEB server key to client

Once this has been done.

Step 8 – Enrolment/Registration page

The client is hyperlinked to the Enrolment/Registration page where they re-enter/or confirm their personal data, credit data, email data, etc. Note: The data entered by the user will never ever have to be entered

again, as all of the information provided will be stored in the VirtualSAFE. Once the user has completed entering their information:

Step 9

- A VirtualSAFE certificate will be created for the user
- The user's data and the user's VirtualSAFE certificate will be stored to the Secure Data Repository.
- All of the user's VirtualSAFE data will be stored to the VirtualSAFE x500

Step 10 – Confirmation to the user

Would you like to enroll with VirtualSAFE? NO

Step 11 – The enabler

The user has become a registered and authenticated VirtualSAFE user and can now shop anywhere on the net, their information is stored in encrypted form to Oracle, our any database, etc., and an email of registered confirmation is sent to them, as well as a cancellation procedure.

CA Processes. FIG. 12 is a flowchart indicating CA processes. The steps to be followed are as per Certificate Policies (CP) and Certificate Practice Statements (CPS).

Enrolment Policy. Procedures for handling incorrect PIN or mistyped PIN are handled in accordance to VirtualSAFE Policy and/or Merchant/Business Policy.

Referring again to FIG. 1, certain components the VirtualSAFE invention will be described in more detail in the following.

Public Key Infrastructure 101. The Public-Key Infrastructure (PKI) arrangement deployed in the VirtualSAFE invention consists of multi-tiered and distinct Certificate Authorities defined as follows:

1. An External Certification Authority ("ECA") designated to issue web certificates to user client computers. Therefore, each user will have an ECA key pair as follows:
    - ECA Public Key ("ECApub")
    - ECA Private Key ("ECApriv")
2. An internal VirtualSAFE Certification Authority ("VCA") designated to issue corresponding internal VirtualSAFE certificates for each external user web certificate. Therefore, each user will have a VCA key pair as follows:
    - VCA Public Key ("VCApub")
    - VCA Private Key ("VCApriv")

3. The VCA will issue an encryption certificate to the VirtualSAFE Web Server (VWS) with the following key pair:

    - VSW Public Key ("VSWpub")
    - VSW Private Key ("VSWpriv")

Recall that VirtualSAFE has an Attribute Authority (AA) designated for managing access and network permission attributes for users.

Redirection Link 102. The Redirection Link (RL) process enables an online e-commerce process to access the VirtualSAFE secure transaction environment. The process consists of the following steps:

1. The user completes the required conditions for executing a transaction, or request for a resource, by selecting and retrieving the appropriate access query page from a merchant server.

2. The access query will be in the form "buy now" for a payment transaction or "access now" for a secure resource access or retrieval.

3. The Redirection Link (RL) will capture the relevant data from the merchant server and redirect the contents of the request to the VirtualSAFE. In the case of any transaction/access any amount/session unique identifier may be transferred. In the case of a resource access request, user attributes may be transferred to the Virtual SAFE.

The redirection link allows non-repudiation by using X.509 certificates and a secure algorithm and protocol residing on a remote merchant, business, or resource site. The redirection request, once processed, initiates the Secure Remote Pointer (SRP) process for encrypting, signing, and hashing transferred data. The SRP is described in the following section. Merchant and/or user can digitally sign the transaction.

Secure Remote Pointer / Plug-In / Application 103. The Secure Remote Pointer (SRP) is a VirtualSAFE compatible application that runs as a web browser plug-in, applet, or standard application. The client browser, to conduct secure communications with VirtualSAFE, uses the SRP. The process is initiated when the user clicks on a redirection link (RL) that requires an authentication and authorization check. Clicking on this RL, as described above, implies a commitment to access a resource, for example, a payment transaction or a secure database. In order to execute a transaction, authentication of the user is required. The process requires authentication of the user computer via an X.509 Digital Certificate or other standard PKI format. Once authenticated with a digital certificate the user, application, or browser will always communicate with VirtualSAFE via the secure web browser plug-in or the SRP or application. The security approach to the SRP includes multi-layer security via encryption and enveloping techniques. The SRP functions include encryption of data that will be packaged and then encrypted via secure sessions in addition to an SSL communication channel with the VirtualSAFE database to complete transactions and store operational data, or for other accesses purposes.

Referring to FIG. 2, which is a block diagram of the secure remote pointer **103**, the method used will now be described. In order to securely capture and store data from the customer, the following steps and requirements are incorporated in the SRP:

1. The entire communication will take place over a client-server in addition to an authenticated SSL channel. Two-way authentication is established using the digital certificate distribution method described above.

   a) The SRP will encrypt data being transmitted to the VirtualSAFE prior to being in an electronic envelope. The envelope in turn will be transmitted over the secure session in addition to an SSL channel protocol. (Encrypted data is sent in accordance with VirtualSAFE policy through the SSL.)

   b) The VCA Public-key, VCApub, of the user that is stored in the browser, application, message, or cookie is used to encrypt data once, creating C1 **201**.

   c) A time stamp is concatenated to the encrypted data package C1 **201**, the ECA private key, ECApriv, belonging to the user signs the data to create C2 **202**.

   d) The result is encrypted with the VirtualSAFE Web Server Public-key (VSWpub) to create C3 **203**. This key can be obtained by the SRP or in case of dynamic application that will be transmitted with an ActiveX Control / Java Applet / Application /, etc., at the time of page initiation.

2. Encryption and signing of the data package is completed entirely within the secure confines of the SRP. The following steps are carried out to securely communicate with the VirtualSAFE.

   a) C3 **203** is transmitted as C4 **204** over SSL or other secured channel encrypted with the appropriate session keys.

   b) The data package C4 **204** is decrypted **205** by the reciprocal SSL, or secure channel session keys, at the VirtualSAFE Web Server to reveal C3 .

   c) The VirtualSAFE Web Server/Application will decrypt **206** the data package with its private key VSWpriv locally on the Web Server to reveal C2 (optionally by a VirtualSAFE Application behind the Web Server).

   d) The data is now ready to be used locally within the VirtualSAFE.

   e) The data package C2 is passed **207** to the User's VirtualSAFE Deposit Box.

3. The data package in its new form may now be used by the VirtualSAFE for various different operations including:

   a) Authentication. Data received at authentication will be treated as an encrypted quantity that does not need to be decrypted. The encrypted data will be compared with a database of encrypted PINs in the VirtualSAFE: (i) Identification rolling prefix * possible encrypted will

be checked with policy manager and requested for validation; and, (ii) Validation result will proceed with transaction or terminate session.

b) Transaction. The VirtualSAFE private-key VCApriv of the Customer will decrypt transaction data received at the time of purchase. The encrypted private information of the customer in the customer repository will be decrypted and hashed or encrypted, or digitally signed and sent to the payment processor, or other transaction engine: (i) The VirtualSAFE Private-key VCApriv will be used to decrypt the local Customer Credit information for the transaction. The Credit information will then be passed to the payment processor or other transaction engine. The information may be optionally signed by the customer, hashed or encrypted by administrator. Payment set up will define future process and necessary encryption or digital signing set of information.

Referring again to FIGURES 1 and 2, the method of decryption and of searching for VirtualSAFE Deposit Box **115** information will be addressed in following descriptions of the Virtual Identity **105**, Virtual Smart Card **106**, and other components of the invention.

Virtual Identity 105. The VirtualSAFE Virtual Identity (VI) process involves the use of X.509 Digital Certificates in the internal VirtualSAFE Certification Authority (VCA), as described above. The Virtual Identity (VI) may include the following:

1. The Web certificate from a third party or ECA public and private key of the user:
    - Public Key (ECApub)
    - Private Key (ECApriv)
2. The VirtualSAFE CA public and private key of the user:
    - VCA Public Key (VCApub)
    - VCA Private Key (VCApriv)
3. The private data of the user is encrypted with the user's public key VCApub key and committed to the local database.
4. The user's Private Key VCApriv is stored securely elsewhere in VirtualSAFE.
5. VirtualSAFE then executes a retrieval of the information in the Virtual Identity by employing a composite secure algorithm and protocol described below in conjunction with the Virtual Smart Card component. The retrieval and storage of the secure data is designed on the principle of secret, shared secret, and physical material.
6. The user data stored in the Virtual Identity may include the following:

- Encrypted PIN and other access data
- AA Reference Data
- Personal User Data
- Financial User Data

Attribute Authority 104. The implementation of a remote electronic commerce application requires managing access to electronic resources. The core value of a commerce application lies in the ability to manage identities and the associated privileges attached to these identities. In traditional approaches to PKI, a Certification Authority (CA) issues and revokes certificates used to bind a name to a public key. However, the existing certificate structure requires an existing name space where each individual is uniquely identified with a unique name and often a unique number. In commerce transactions, the merchant server may be assured of the customer identity by means of the digital certificate verification. However, the authorization of the customer identity to actually perform the transaction (or other access privilege) is not necessarily a given. A required enhancement to the process is a means for the merchant to be certain that the actions to be undertaken are legally binding and the signer indeed has the authority to execute them.

The use of a digital certificate is augmented from the basic capability of a digitally signed testimonial to the validity of the public key it contains, by including attributes that provide or grant some privilege to its owner. The benefit of this approach makes the attribute certificate well suited for access control to a system or some other method of authorization control.

By definition, access control entails the limiting of activities of a user on the system. Enforcement of such controls is accomplished by maintaining a reference monitor that mediates access attempts by consulting an authorization base to determine if the user attempting the access is authorized to do so. A distinction is made here between authentication and access control, wherein authentication merely confirms the identity of the user, while access control establishes identity privileges on the basis of successful authentication.

Access control may be deployed in one of two modes, namely, an activity-based mode or a group-based mode. In the activity-based mode, user access control is managed according to activity monitoring where each access is checked against an authorization table and permissions are granted or denied on that basis. In the group-based mode, user access control is based on the group to which a user belongs. Users of the same group are authorized to perform a specific set of system tasks or actions. Instead of specifying all the individual user authorizations, actions are assigned according to the group where any individual user may accomplish the same tasks in its group.

Group-based access control is characterized by the following:

1. Authorizations are defined according to classes of objects or resources where a member of a group may be authorized to access a particular resource. This enables a class of resources to be accessible to a group of users without specifying individual resource access privileges.

2. Access to specific resources, are defined by the activities required by a particular group. A group is defined by its authorizations and a user may be afforded access rights according to a group designation.

3. Groups may be nested in a hierarchical order wherein higher-class groups may inherit lower-class group authorizations.

4. Minimum access may be granted on the basis of a minimum group characteristic. Access for lower risk resources may be afforded by assigning a lower class role.

5. Access privileges can be specified according to Boolean constructs wherein several group authorizations may be afforded to a user to achieve a composite access portfolio.

A group-based model is advantageous on several levels. For example, overall administration is removed from individual user access management and is migrated to the group level.

There may be of several authentications for a user including the following:

- User authentication as described by the Authentication Authority. In addition, an enrolment value is exchanged between VirtualSAFE and a secure portal with a resource group. Any transaction/access session is performed by a minimum of two channels simultaneously (e.g. SSL and VPN, etc.), combining enroll value and session value digitally signed by

all parties based on a digital identity group (i.e. secret, shared-secret, physical material).

- Account/Resource Digital Signature Authentication based on the principle of a digital signature verified by a user public key attached to the Account/Resource.

Attribute Certificates. The digital certificate infrastructure is well suited for this approach to access control. In the standard digital certificate, a public key is signed by a Certification Authority (CA) and distributed for authentication purposes. The same principle is applied to group-based access control. In this method, a group is described by a set of attributes that enable the members of the group to perform common functions. The attributes are bound together by a digital signature by a CA, creating an Attribute Certificate (AC), which is consequently unalterable until a new set of attributes is designated and signed. The Attribute Certificate may contain the following fields:

- Version: Designates format of the AC currently in use.
- Subject: Context of the AC usage in terms of the given application.
- Issuer: Issuer of the certified AC.
- Digital signature: Digital signature of the AC data by the Issuer.
- Issuer Unique ID

- Serial Number: A unique identifier of the AC.
- Expiry: Defines the validity period of the AC.
- Attributes: Access control definitions for the AC.

Attribute Authentication Authority 104. The Attribute Authentication Authority implementation represents a key innovation in the authentication and authorization business processes. Existing business processes already use some means of account-based protocols to evaluate attributes. However, these methods are reliant on a knowledge factor authentication where the user divulges some previously agreed secret, that is, a "shared secret".

Current business processes supporting authentication are primarily "shared-secret" based (e.g. PINs, mother's maiden name, SIN#, SSN#, etc.). The "shared-secret" has the disadvantage that the shared-secret can both originate as well as authenticate a transaction (i.e. existing business infrastructures need extra levels of security to prevent divulging the shared secret). Upgrading these existing authentication business infrastructures to PKI is straightforward and eliminates the vulnerability associated with divulging the authenticating value. Furthermore, these are integrated to produce robust authentication business processes (i.e. as compared to the certificate design point for offline email which had no authentication infrastructure). In other words, the existing financial business processes for managing authentication material can be leveraged for managing public key authentication material.

The VirtualSAFE invention includes a straightforward upgrade to all existing "shared-secret" authentication business processes, that is, upgraded from "shared-secret" to secret, shared-secret, and physical material representing digital certificates and signatures using existing business processes. By including an Attribute Certificate in a transaction, the authentication of the user is augmented immediately by identifying the authorization of the user to activate payment. The following is one embodiment of an access control system in accordance with the invention:

1. A Trusted-Third Party Certification Authority CA(x)
2. An Authentication Authority AA(y)
3. Organization Resource R(1) , R(2) , R(3) , R(4) ,... R(n)
4. Groups described by attributes G(1), G(2), ...G(n)
5. Users designated as U(1), U(2), ... U(n)

The Certification Authority CA(x) is capable of issuing public key certificates and of signing the root issuing certificate of the Authentication Authority AA(y). Resources are classed and labeled such that access to resource R(1) is distinct and non-connected with R(2), or any other resource R(n). Each group G(n) is assigned authorization to access a particular set of resources based on policy, for example, G(1) may access R(1), R(3), and R(4).

In this embodiment, a method by which an authorization environment for resource access is made instantaneous, may include the following steps:

1. The root certificate CA(x) is distributed to all users U(n) and resources R(n).

2. The root certificate AA(y) is also made publicly available.

3. Authentication Authority AA(y) is able to issue ACs to all users U(n) in G(n).

To exercise a resource access authorization, the following steps may now be followed:

1. An access request to resource R(1) is made by a user member U(1) of group G(1), where G(1) is granted access to R(1), R(2), and R(4), and is digitally signed by the user.

2. Resource R(1) verifies the digital signature of U(1) with U(1)'s public-key certificate.

3. Resource R(1) checks the validity of U(1)'s certificate by verifying the digital signature with CA(x)'s root certificate.

4. The AC of U(1) is verified using AA(y)'s root certificate.

5. The attributes in U(1)'s certificate are then used to grant access, according to the group membership of U(1), to G(1) which includes R(1) access.

Given the successful verification of these queries on U(1)'s AC, then the result will be either to deny access or to grant access on the basis of identity authentication and appropriate access authorization.

Virtual Smart Card 106. The Virtual Smart Card (VSC) is a VirtualSAFE internal application that acts as a local secure proxy to an external virtual authentication token accessed via the Secure Remote Pointer (SRP). The VSC authenticates, encrypts and decrypts VirtualSAFE user data using a multi-tiered Public Key Infrastructure (PKI) managed service. The VSC implements a multi-tiered PKI by designating a dual set of key pairs for each user. The first set is an External Public-Private key pair, issued by the External Certification Authority (ECA), which resides on the client or web browser and interoperates with the SRP. The second set is a local VirtualSAFE Public-Private key pair issued by the VirtualSAFE Certification Authority (VCA) that resides securely and inaccessibly to the outside network within the VirtualSAFE. The Virtual Smart Card (VSC) is part of a secure backend Virtual Identity management system. The system includes the following:

1. Client Terminal. The client terminal consists of a personal computer or device, network interface communication capability, and World Wide Web browser application. The client terminal will run the Secure Remote Pointer that makes a secure connection with the Web server.

2. World Wide Web Server. The Web Server consists of a server (World Wide Web or other front-end system server) configured to serve web

pages. The Web Server can serve pages related to a commerce shopping-cart application or serve pages related to access of controlled resources such as documents or other applications.

3. VirtualSAFE. The VirtualSAFE server embodies the VSC capability and the requisite VirtualSAFE Deposit Box containing Virtual Identities.

4. Fulfilment Resource. The Fulfilment Resource server is in contact with the VirtualSAFE and may consist of any valuable or sensitive services or systems, including but not limited to payment servers, secure data repositories, or other information.

The method by which the VSC is accessed by the remote client terminal and by which it executes an online interaction may be outlined as follows:

1. A communication channel is opened between the client terminal and the web server. The client terminal is presented with the User content from the server and the user will browse for items and complete the User access decision. In the case of an e-commerce application, this would be equivalent to browsing an electronic shopping cart application and composing a list of items for a purchase decision.

2. Upon completion of the user's resource access decisions, the online application is ready to complete the transaction by final choice in the selection process. A signal to actuate a resource access process on behalf

of the user is transmitted when the customer clicks the Redirection Link on the server resource decision web page.

3. The World Wide Web server communicates the requirement to execute resource access to the VirtualSAFE over a secure channel whereby authentication is initiated between the client terminal and the VirtualSAFE.

4. The VirtualSAFE initiates the Virtual Smart Card (VSC) authentication by immediately downloading the Secure Remote Pointer (SRP) to the client terminal.

5. The SRP requires PIN and PIN authentication from the user.

The VSC component of the VirtualSAFE invention includes a multi-tiered authentication mechanism that consists of the elements listed previously in the description of the Public Key Infrastructure (PKI), that is, the ECA, VCA, and AA.

The method for initiating the VSC may include the following:

1. A User VCA Public-Private key-pair will be generated by the VirtualSAFE and stored as follows:

    a) The VCA Public-key, VCApub, will be combined with the Certificate Digital Signature from the External Public Key Certificate, ECA, and used as a unique identifier or footprint.

b) This combined unique identifier and digital certificate data, as per the VirtualSAFE algorithm, will be stored in an online application, browser cookie, or dynamic header of a web page, and automatically downloaded to the client terminal or web browser.

c) The unique identifier and digital certificate data, as per the VirtualSAFE algorithm, will also be stored with the user's Virtual Identity (VI) as stored in the user database. As the database user information is entirely encrypted, the unique identifier and digital certificate data, as per the VirtualSAFE algorithm, will be used as a search index in order to retrieve encrypted information about a particular user.

d) Every query communicated to the VSC from the SRP will contain the user's unique identifier and digital certificate data, as per the VirtualSAFE algorithm, for identification purposes. Note: The data from the SRP is signed and encrypted to prevent fraud.

2. All the user data stored in the VirtualSAFE database is encrypted with the individual user's VirtualSAFE private key VCApriv. Any key that is external to the VirtualSAFE cannot decrypt the local data, for example, the ECApriv key. The VCApriv key is stored securely in the VirtualSAFE, apart from the VSDB.

3. When a query is made via the Secure Remote Pointer (SRP) it can arrive in either of the following two forms (as discussed above):

a) Authentication.The SRP query composed of a data package C1 is decrypted 208 (see FIG. 2) and verified for use by the VirtualSAFE as described above.

I. In this case the data contained in the data package is the user footprint and the verified but still encrypted (with VCApub) Personal Identification Number (PIN) from the remote client terminal.

II. The user footprint is used to locate the VirtualSAFE database Virtual Identity of the particular user.

III. Upon retrieval of the VI of the particular user, the encrypted PIN from the SRP is compared to the PIN in the VI record.

IV. If the encrypted data fields match, then an authentication is affirmed, and Authorizations associated with this VI are requested from the AA.

V. The remaining authorizations are queried and verified as outlined in the previous section on Authentication Authority.

b) Transaction. The SRP query composed of a data package C1 is decrypted and verified for use by the VirtualSAFE as described above.

I. In this case, the data contained in the data package is the user footprint and the verified but still encrypted (with VCApub) resource access query C1 from the remote client terminal.

II. The user footprint is used to locate the VirtualSAFE VSC and Virtual Identity for the particular user.

III. Upon retrieval of the VI for the particular user, the encrypted resource access query in C1 from the SRP is decrypted 109 (see FIG. 2) with VCApriv that reveals message M.

IV. The message M contains formatted instructions for the VirtualSAFE to perform some transaction or resource access.

V. In order to carry out the transaction or resource access the local VI data must be decrypted with VCApriv. Upon decryption of user data, the transaction must be authorized by the AA

VI. The transaction authorization is queried and verified as outlined in the previous section on Authentication Authority.

VII. The transaction or resource access is executed.

VIII. The decrypted VI data is destroyed, and the existing user VI record remains encrypted in the VirtualSAFE Deposit Box.

IX. Results of the transaction or resource access are returned to the VirtualSAFE and the VI record is updated and encrypted/hashed.

X. A confirmation of the transaction or resource access is communicated to the client terminal via the SRP and merchant through dedicated channel or any other type of messaging.

Payment Processing Engine 110. The VirtualSAFE invention's Payment Processing Engine consists of servers and connectivity to a payment gateway wherein the servers support VirtualSAFE's compatible client-server SSL authentication. Payment processing may include the following: credit card payment, debit card payement, direct debit, check processing, wire, and EFT. Payments in VirtualSAFE may be processed by several modes including batch processing and real-time processing. Each mode achieves the same set of possible results from a payment request, whether it is authorized, settled, or declined. Real-time processing is achieved by executing a singular payment request in real-time while the customer is connected. VirtualSAFE's payment processing engine may support several transactions including the following:

- Credit Card Authorization

- Address Verification
- Payment Submission
- Payment Settlement
- Transaction Void
- Transaction Credit

Risk Management Engine 111. VirtualSAFE's Risk Management Engine augments the payment processing functionality by providing intermediate vetting of transactions prior to execution by a remote processor. Credit Risk Management occurs in different scenarios of customer enrolment, management, and payment processing. An individual customer's credit rating is used to determine acceptability of payment transaction processing. This value is collected either at enrolment time or during a profile update. It is retrieved by calling the local database using various information fields belonging to the customer. The risk value returned is stored in the VSDB. At transaction processing time, the credit value rating is retrieved from the VSDB and used to evaluate whether a transaction should be transmitted to the payment processor. VirtualSAFE maintains ongoing transaction logs or a system transaction journal, that is, any transaction (e.g. payment, customer profile modification, etc) executed on VirtualSAFE is stored along with the information identifying the transaction, issuer, date, resources affected, and Registered Resource Site status.

Transaction Fulfilment Mechanism 112. The VirtualSAFE invention's Transaction Fulfilment Mechanism (TFM) consists of a set of fraud management heuristics that are invoked in a progression that leads to a final fulfillment condition. The fulfillment condition will dictate what type of delivery is to be made and the associated criteria for completion. The TFM and fraud management heuristic is comprised of several steps including the following:

1. Customer Authentication Scoring
2. Credential Identification Scoring
3. Transaction Risk Scoring
4. Fulfillment Response
5. Fulfillment Delivery

The first three of these steps are combined to achieve a transaction score that is used to determine the fulfillment response and type of fulfillment delivery. Each step is mutually exclusive and only the combined result matters in achieving the complete fulfillment. The above steps may be described in more detail as follows:

Customer Authentication Scoring. This step is initiated by compiling the browser logon criteria into a composite score. Elements from the browser logon that may be considered include the following:

- Certificate Authentication

- Secure Cookies
- PIN or PIN value
- SRP Verifications
- Other

Credential Identification Scoring. This step creates a composite score based on the identifying elements in the order information. Each are weighted and summed based on various criteria which may include the following:

- Address
- Amount
- Over Limit
- Declined
- Plug-in Verifications
- Risk Assessment
- Transaction type
- Payment type
- Fraud
- Third party assessment proof or change

Transaction Scoring. This step involves computing a value and risk for the actual transaction being processed based on transaction attributes as follows:

- External: Third Party Fraud Assessment that is used for clarification of Internal scoring and adjusts final conclusion and instruction for fulfilment execution.

- Internal: Primary Attribute, Secondary Attribute, Reduction, Tune Up, Risk Adjustment, and Fraud Data Configuration.

Fulfilment Response. This is the required response to the established criteria. The transaction will be treated as a variant of "card present", where the physical credit card is actually present, or "authorization", where the credit issuer must confirm available credit.

- Card Present V

- Card Present R

- Authorization

Fulfilment Delivery. This is the resulting action taken on the composite score after all of the scoring attributes are evaluated and checked. The resulting delivery may include the following:

- Request for signature

- Drop off
- Delivery
- Signature
- Photo ID

Draw Request Messages. A detailed description of one method for processing a draw request message in conjunction with a virtual smart card is presented in the following.

Once a draw request message has been received by the payment server and passed along to the terminal, the terminal parses the message back into individual responses and passes these responses sequentially to the virtual smart card. In an alternative embodiment, a dumb terminal is used and the draw request is parsed into its components and otherwise processed by the payment server, which then sends the responses to the virtual smart card itself.

The payment code module of the payment server edits the draw request for syntactic correctness and logs the draw request message as being received. The draw request is passed to the terminal interface of the payment server. In one embodiment, the terminal interface then requests a terminal from the payment server's terminal pool. The payment server may have a pool of terminals connected to a terminal concentrator that is established at start-up. At start-up, the payment server receives a

list of all valid terminal identifiers. The payment server uses these identifiers and its knowledge of transactions in progress to determine an appropriate terminal to process the transaction. Once a terminal is determined, the terminal interface builds a terminal specific message based upon the draw request and the type of terminal.

The terminal specific draw request is sent to the chosen terminal over a local area network. A concentrator may act as a router between a transaction thread in the payment server and a corresponding terminal if many terminals are attached to the payment server. The concentrator looks at a header on the draw request to determine to which terminal the transaction should be routed. In one embodiment of the invention, the concentrator is not necessary and the payment server communicates directly with the terminal.

The terminal parses the draw request message into its various components and processes each component in turn to emulate a card interacting with the virtual smart card in a physical terminal. Prepackaging of a variety of data into the draw request message results in fewer exchanges over the Internet between the VSAA server and the payment server. By now simulating an interaction, the virtual smart card behaves as if it were in a physical terminal along with an actual smart card. A variety of responses from a smart card may be emulated. In one embodiment, the terminal sends each of the two commands "Answer to Reset" and "Initialize IE-W for Purchase" down to the virtual smart card individually and waits for a return message, "Debit IE-W," before sending the next response. For a public key transaction, the certificates read by the client are also included as individual responses. In this way, even though all of the smart card information (the draw request) originating from the VSAA server

has been sent at once in prepackaged form over the Internet, the interaction between the smart card and virtual smart card in a physical terminal is simulated at the terminal in a remote location.

The terminal reaches a "draw amount" state, indicating that the virtual smart card is able to generate a debit command. The virtual smart card generates its virtual smart card digital signature and the command "Debit IE-W". The digital signature and debit commands are sent to the terminal. The debit command issued by the virtual smart card may contain a wide variety of information including the virtual smart card identifier, the transaction identifier, the amount to be debited, the currency and currency exponent for the amount, the virtual smart card digital signature, the date, time, and location. The terminal in turn sends the digital signature, command, and the terminal identifier to the payment server.

Database Repositories (DR). VirutalSAFE has the following two Database Repositories (DR):

1. VSC/Customer Database. This DR is controlled by VirtualSAFE and contains Customer Virtual Identities (VI).

2. VSC/Merchant Repository. This DR is controlled by VirtualSAFE and interfaces with a designated payment processor (or other fulfillment resource).

The VSC/Customer and Merchant Repositories are interlinked based on the business rules and policies defined according to business requirements. The VSC/Customer Repository is a composite of the Customer VI records. These records include all personal, financial, and credit data belonging to each customer.

VSC/Merchant Repository is based on a fixed schema developed for payment and contains all the data profiles belonging to merchants. The VSC/Merchant Repository also contains payment transactions in various states of completion with the credit payment processor. These states may include the following:

- Validated
- Failed
- Settled

These states may be managed, voided, cancelled, etc., and queries, such as retrieving transaction history, return various responses including transaction content which may include the following:

- Payment server Transaction ID
- Credit Card Number
- Expiry Date
- Amount
- Transaction Date

- Transaction Status

The financial infrastructure is securely interfaced with VirtualSAFE such that all transaction communication is digitally encrypted and signed.

Having described the various components that comprise the VirtualSAFE invention, an overview description of VirtualSAFE's method of operation and the use VirtualSAFE's Virtual Smart Cards will now be provided as follows.

Method of Operation. Through VirtualSAFE's implementation of an AA, multiple entities may inter-operate on an open and non-trusted network by means of AC access control. VirtualSAFE permits electronic payment, credit collection, and secure remote fulfillment processes. Through the use of the Virtual Smart Card, Secure Remote Pointer, Attribute Authority, and other components, VirtualSAFE may be implemented in a variety of ways. Modularity of security objects and application objects enable VirtualSAFE to be applied to numerous electronic commerce environments. In VirtualSAFE, an electronic inter-networking payment system provides for transactions using an electronic payment VSDB that is customarily used for keeping money, credit cards, and other forms of payment organized. Access to the instruments in the wallet or purse is restricted by a sophisticated encryption and authentication method to avoid unauthorized payments. A successful cryptographic

authentication is required in order to obtain access to the VSDB. The authentication protocol obtains the information necessary for creating a network session granting authority to utilize an instrument, a payment holder, and a complete electronic wallet. Electronic approval results in the generation of an electronic transaction to complete the order.

Use of Virtual Smart Cards. VirtualSAFE's Virtual Smart Cards (VSC) may be used in the context of a Point of Sale (POS) card-swipe terminal at a retail outlet, as follows. Assume that the customer maintains an account with an existing financial institution. The following steps may be included in the use of the VSC:

1. The Merchant swipes the magnetic stripe customer debit or credit card at the POS.

2. The POS transmits a request for authorization through the financial network, where a connection is made to an intermediate smart card reader and device on the premises of the Merchant.

3. The smart card reader and device is occupied by the Merchant's smart card.

4. The transaction authorization from the POS prompts the smart card reader to encrypt and sign the data prior to transmission.

5. VirtualSAFE requires a PIN identification to authenticate the customer.

6. VirtualSAFE performs an authentication of the customer using the Virtual Smart Card methodology (as described above).

7. The customer is authenticated.

8. The VirtualSAFE sends an encrypted or digitally hashed and signed transaction to the Financial Institution or Interac switch.

9. An authorization is returned to the VirtualSAFE or to the Merchant.

10. The authorization is decrypted by the smart card reader and device.

11. The message of authorization is returned to the POS terminal.

The Virtual Smart Cards (VSC) may also be used in the context of check processing, as follows. Assume that the customer is already enrolled in the VirtualSAFE. The following steps may be included in the use of the VSC:

1. The customer requests a payment be made to a Merchant using a VirtualSAFE check by clicking the appropriate Redirection Link (RL) on a merchant web site.

2. The customer is forwarded to the VirtualSAFE.

3. VirtualSAFE performs a remote authentication of the user and passes the customer to their VSC.

4. The customer approves a check payment from their financial credit personal portfolio.

5. VirtualSAFE signs the data request and sends it to the financial institution.

6. An optional printout of the check is generated inside the physically secure facilityies of the financial institution.

7. VirtualSAFE receives confirmation of the check status: processed, returned, NSF, etc.

8. VirtualSAFE encrypts and stores the transaction data in the customer's Virtual Identity.

9. An optional message or printout of the customer transaction is forwarded to the customer or merchant.

Referring to FIGURES 13 through 31, to reiterate and expand, components and processes within VirtualSAFE include the following.

Participants. Referring to FIG. 13, there is shown a block diagram of the participants and their contractual relationships in VirtualSAFE. The electronic commerce environment requires significant security and auditing processes bound to the actual business operations and processes. Accordingly, the primary concerns are the

contractual relationship between parties, the enforcement of the business policy, and the transparency of the processes.

1. VirtualSAFE Business Policy. Within the VirtualSAFE Business Policy there are three main components that that will never be compromised and they are: Privacy, Security, and Ease of Use.

- Privacy: The securely structured attributes that are handled and covered under the Privacy aspect of the VirtualSAFE Business Policy include:
  - ACCESS And PRIVILEGES. In VirtualSAFE, only the user has access to their private information.
  - Compliancy And Standards. VirtualSAFE adheres to the World Privacy Regulations and Standards.
  - Higher Power Rule. In VirtualSAFE, Third Party access to private and personal information can only be granted by Court Order. This signifies the only time when a user's private information can be attained other than by the user.
- Security: The securely structured attributes that are handled and covered under the Security aspect of the VirtualSAFE Business Policy include:

- International Security Standards. VirtualSAFE follows all international standards for the security within x500 directories and is 140 FIPS/3 Complaint.

- Monitoring, Support And Control. VirtualSAFE is comprehensively monitored 24 hours per day, 7 days per week. There is no shutdown time and support is readily available if required.

- Remote Virus Scan. VirtualSAFE is continuously being upgraded with new virus protection directly and remotely to ensure the optimum in service, and security structure. As a leading technology in e-commerce secure systems, VirtualSAFE provides their users with the confidence that their information is secure from any virus and/or unwelcome invasion.

- Ease of Use. The securely structured attributes that are handled and covered under the Ease of Use aspect of the VirtualSAFE Business Policy include:

  - User Experience. VirtualSAFE does not change the experience of the present user meaning that the user already has the basic skills that are required in order to use VirtualSAFE.

- Info Entered Once. In VirtualSAFE, the user only has to input their private and personal information once, and then it is stored in the VirtualSAFE. Every time they login afterwards, their identity and credit attributes are linked to their digital ID.

- Click-And-Go. VirtualSAFE users experience Click-and-Go from any VirtualSAFE site. Their digital IDs are recognized everywhere and they can jump from site to site quite easily.

2. Business Policy (Third Party). VirtualSAFE has the capability, and complies to other businesses' business policies, so as not to comprise their way of doing business.

Enrolment. Referring to FIG. 14, there is shown a block diagram of the enrollment process in VirtualSAFE. VirtualSAFE registers users' personal data (i.e. credit card information) once. Data pertaining to their enrolment, authentication, and reference is contained within VirtualSAFE. The User is issued a digital ID so that the user never has to enter their data online again. Enrolment data is stored securely in VirtualSAFE under a strict policy.

1. Enrolement in VirtualSAFE. In VirtualSAFE, there are four enrolment levels: resource enrolment, customer enrolment, attribute resource enrolment, and employee enrolment. With respect to employee enrolment

levels, two controls are established, both locally and remotely: IT Access Control and Physical Access Control.

2. VirtualSAFE Customer Authentication Enrolment.Within VirtualSAFE, customers are authenticated using their digital IDs.

3. User Authentication. Within VirtualSAFE, the users are authenticated using their digital IDs.

4. Reference Validation. If for some reason there is a problem in recognition, then reference validation is the next step used to authenticate the user, customer and/or resource.

Online Transactions. Referring to FIG. 15, there is shown a block diagram of the online transaction process in VirtualSAFE. VirtualSAFE operates as an authentication layer or authentication authority between the user, the terminal and the VirtualSAFE server. Through a multi-tiered authentication mechanism, the remote user is queried and authenticated to produce smart card emulation as if the physical card was present.

1. Customer Browses Site. In VirtualSAFE, customers using their digital certificates enables them to browse their online banking sites and use the smart card application.

2. Secured And Authenticated Access. Once the user/employee/customer has been authenticated in VirtualSAFE, they have access to online banking, the online brokerage, account data aggregation reports and audit

performance, and online payment transaction requests; such as credit/debit card, electronic check, wire transfer, etc. They also have access to a VirtualSAFE Deposit Box (VSDB).And finally, the users have access to other valuable services such as the following:

- Secure e-mail
- Logistics support for individual, small and medium-sized businesses.
- An application front-end that is easy to understand and use.
- Application accessible through the inter/intranet.
- VirtualSAFE is interoperable with existing professional or custom applications.
- Secure collaboration place.

Server Authentication. Referring to FIG. 16, there is shown a block diagram of the server authentication process in VirtualSAFE. The Secure Remote Pointer (SRP) is a VirtualSAFE compatible application that runs as a web browser plug-in, applet or application. The SRP is used by the user browser client to conduct secure communication with VirtualSAFE. This process is initiated when the user clicks on a redirection link (RL) that requires an authentication and authorization check. The SSL Server Authentication is established as follows:

1. VirtualSAFE Server Initiates One-Way SSL Handshake With User.

2. Server Authentication. The server is then further authenticated as VirtualSAFE stores the transmitted information and queries the received digital certificate.

Computer Authentication. Referring to FIG. 17, there is shown a block diagram of the computer authentication process in VirtualSAFE. The VirtualSAFE Virtual Identity (VI) process involves the use of a PKI Digital Certificate. The Virtual Identity (VI) includes the following:

- A Web certificate from a third party or ECA public and private key of the user.
- Authentication is initiated over a secure SSL channel

Computer Authentication is established as follows:

1. VirtualSAFE Server Initiates a One-Way SSL Handshake.
2. Digital Certificate (PKI) Establishes a Two-Way SSL Handshake. The two-way SSL handshake ensures that VirtualSAFE interoperability functions properly, VirtualSAFE is X509 compatible with Entrust, Baltimore, Verisign, etc., VirtualSAFE second phase is EC^2 compliant (Certicom), and that VirtualSAFE is compliant with other PKI standards (i.e. Meta, etc.).

3. By Verification of X500 Global Directory. VirtualSAFE is fully capable of determining certificate authenticity by verifying public directories (e.g. Entrust, Baltimore, Verisign, etc.).

User Authentication. Referring to FIG. 18, there is shown a block diagram of the user authentication process in VirtualSAFE. The entire communication will take place over a client-server authenticated SSL channel establishing two-way authentication using digital certificate distribution. Encryption and signing of the data package is completed entirely within the secure confines of the Secure Remote Pointer (SRP). The user data stored in the Virtual Identity may include the following:

- Encrypted PIN and other access data
- Authentication Authority (AA) reference data
- Personal User Data
- Financial User Data

Once the user data has been stored within VirtualSAFE, the following steps may take place to ensure that the user is authenticated:

1. Virtual SMART CARD (VSC) is activated. A remote virus check is performed and an optional keystroke is checked and the VirtualSAFE certificate application is validated.
2. VirtualSAFE Secure Plug-In / Application Activated.
3. User Presents Identification Strings.

4. Virtual Smart Card Identifies User in VS X500 Directory.

5. User's Pin And Timestamp are Triple Encrypted - Digitally Signed.

6. VirtualSAFE Decrypts Digitally Signed User's Pin And Timestamp.

7. User Encrypted Pin Is Validated by VirtualSAFE.

8. VirtualSAFE Encrypted Prefix Validated by Supervisor.

9. VirtualSAFE Proceeds with Back-End Authentication.

Back-End Authentication. Referring to FIG. 19, there is shown a block diagram of the back-end authentication process in VirtualSAFE. The VirtualSAFE Payment Processing Engine consists of servers and connectivity to a payment gateway. The VirtualSAFE Risk Management Engine augments the payment processing functionality by providing intermediate vetting of transactions prior to execution by a remote processor. Credit Risk Management occurs in different scenarios of customer enrolment, management, and payment processing. An individual customer's credit rating is used to determine acceptability of payment transaction processing. For back-end authentication, the following six steps are included in the authentication process:

1. Risk Management. Score value verifications are done both internally and externally and VirtualSAFE stores the assessment result.

2. Insurance Module – Policy Adjustment Limit.

   - Business Liability Policy – Transaction Value

- User Liability Policy – Limited by Credit Worth

3. Messaging – E-Mail or Notification

   - Internal – Business Unit or Administrator

   - External – Business Partner or User

4. VirtualSAFE Encrypted Transaction Log. An encrypted transaction log that stores all transaction records going through the VirtualSAFE.

5. Policy. Three policies are used in back-end authentication: PKI Policy (PC and PCA) as regulated by standard procedure; VirtualSAFE Privacy and Business Policy; and, Third Party Business Policy.

6. Fulfillment Procedure. The fulfillment procedure for back-end authentication is just that, a fulfillment. Authentication of transactions, communications, data storage, access control, administration, and VirtualSAFE value-added services is completed.

Fulfillment. Referring to FIG. 20, there is shown a block diagram of the fulfillment process in VirtualSAFE. The VirtualSAFE Transaction Fulfilment Mechanism (TFM) consists of a set of fraud management heuristics that are invoked in a progression. The fulfilment condition will dictate what type of delivery is to be made. The TFM and fraud management heuristic is comprised of the following steps:

1. Customer Authentication Scoring

2. Credential Identification Scoring

3. Transaction Risk Scoring

4. Fulfilment Response

5. Fulfilment Delivery

The transaction fulfilment mechanism (TFM) assures the following:

- Secured transactions
- Customer and merchant audits
- Customer and merchant liability insurance
- Transaction value insurance
- Fraud control
- Delivery control
- Loyalty program

In assuring these items, the transaction fulfillment mechanism (TFM) allows for the following payment types to be performed:

- Online credit card payment
- Debit card payment
- Electronic check
- Wire

- Electronic transfer of funds
- Coin payments
- Stored-value cards

The transaction fulfillment mechanism (TFM) also provides the following services:

- Data storage
- Secure e-mail
- Logistic support for individual, small and medium size businesses including the following features: an application front-end that is easy to understand and that is user friendly; the application is accessible through the internet/intranet; and, VirtualSAFE is interoperable with existing professional or custom applications.
- Secure collaboration place

Attribute Authentication Authority. Referring to FIG. 21, there is shown a block diagram of the attribute authentication authority process in VirtualSAFE. By definition, access control entails the limiting of activities of a user on the system. Enforcement of such controls is accomplished by maintaining a reference monitor that mediates access attempts by consulting an authorization base to determine if the user attempting the access is authorized to do so. A distinction is made here between authentication and access control, where authentication merely confirms the identity

of the user, while access control establishes identity privileges on the basis of successful authentication.

Virtual Identity (VI). Referring to FIG. 22, there is shown a block diagram of the virtual identity (VI) process in VirtualSAFE. User identity authentication is initiated for each individual transaction by triggering a multi-tiered algorithm that employs Virtual Smart Card technology to interface with standard PKI. Authentication is only possible when the user's personalized "virtual smart card" allows VirtualSAFE to access the respective "virtual identity".

1. Virtual Identity (VI) Private Information. VI is used to create and maintain encrypted data from source data based on provided and validated information.

2. Virtual Identity (VI) Secret Information. VI maintains this information that is encrypted and accessible only to a single user. Only the user knows secret information whose secret it is.

3. Virtual Identity (VI) Shared Secret Information. VI maintains this information that is encrypted and accessible only to the user and the VirtualSAFE proxy. Secret information is known only by the user whose secret it is and by the VirtualSAFE proxy.

4. Virtual Identity (VI) Physical Material. Physical material could be represented by digital certificate or a unique software code (e.g. script,

program or special code). Physical material may include the following: Local, Digital Certificate (Personal Computer, Computer and/or Web Digital Certificate, Smart Card, Magnetic Card or any device operated by the user); VirtualSAFE Certificate (Digital Certificate is a Digital Certificate stored in any type of Repository or VirtualSAFE Repository managed by VirtualSAFE); and, Unique Identifier (Identifier issued uniquely to a user). Technological standards may include the following: Encryption Basis (RSA, CEV and other types of algorithm) and Public Key Infrastructure (PKI, X500, META, etc.).

Virtual Smart Card (VSC). Referring to FIG. 23, there is shown a block diagram of the virtual smart card (VSC) process in VirtualSAFE. The Virtual Smart Card (VSC) is a VirtualSAFE internal application that acts as a local secure proxy to an external virtual authentication token accessed via the Secure Remote Pointer (SRP). The VSC authenticates, encrypts and decrypts VirtualSAFE user data using a multi Public Key Infrastructure (PKI) managed service. The VSC implements a multi-tiered PKI by designating dual sets of key pairs for each user: one External and one Internal Public-Private key pair.

1. Virtual Smart Card (VSc) Functions

- The Virtual Smart Card is the emulation base of the reader and the smart card on a remote location.

- The Virtual Smart Card is used to authenticate user access.
- All information belonging to enrolled members is stored and protected by a proprietary encryption scheme using a high-speed hybrid approach.
- The Virtual Smart Card coordinates the privacy policy.

2. VirtualSAFE Digital Certificate (DC) Repository

- Users remote or roaming digital certificates are stored securely.

3. Virtual Smart Card Authentication

- User authentication using virtual identity.
- User identity is combined of secret, shared secret and physical elements (PKI).

4. Access Portfolio

- Private, Shared, Business or Government.

5. Personal and Financial (P/F) Information

- Personal identity data (e.g. ID, driver's license, address, health card, etc.).
- Financial information (e.g. account numbers, credit/debit card, wire, etc.).

6. Applications

- Remote software licensing.

7. Back-Up

- Transaction logs.
- Transaction revisions.
- Logs.

8. Internal Access

- VirtualSAFE, Private, Shared, Business and Government.

VirtualSAFE Deposit Box (VSDB). Referring to FIG. 24, there is shown a block diagram of the VirtualSAFE deposit box (VSDB) process in VirtualSAFE. VirtualSAFE may also include an ASP (Active Server Pages) module. This will allow a user to access over two hundred news, stock, and information sources. The user can choose from entertainment headlines, custom stock quotes, horoscope and relationship information, health and lifestyle stories, sports scores, news, and much more. To take advantage of these opportunities, the user will need to sign in with a VirtualSAFE VSC (Virtual Smart Card). The VirtualSAFE VSC is a single name and PIN that users can use to sign on to a number of major sites from VirtualSAFE compliant companies. VirtualSAFE uses AA to store the users VirtualSAFE settings, such as the content and colors they would like to see on their VirtualSAFE page.

Users' personal and financial information, and their preferences, etc., are also stored. Since VirtualSAFE uses AA and VSDB to store these settings, the user may view their VirtualSAFE page from any computer connected to the Internet. Also, each member of the user's family with a VirtualSAFE VSC may create and view his or her own personal VirtualSAFE page from the same computer. The user simply has to sign into VirtualSAFE when they visit the VirtualSAFE web site. The user may obtain a VirtualSAFE VSC and learn more about the advantages of having a VSC from a VirtualSAFE web site.

By signing into VirtualSAFE with a VSC, a user will be able to:

- Find out if they have mail or if their friends are online.
- Personalize their VirtualSAFE home page once and view it from any computer, at home, at work, or on the road.
- Choose headlines from popular websites.
- Sign in safely and securely to access their personal settings. The user, and only the user, is the only person who may access his or her choices.

A user may also create a VirtualSAFE VSC test account. To do this, a user must register for a new VirtualSAFE account directly at the domain authority. Once the user's account is created, they will need to sign into a VirtualSAFE VSC Purchase (VVP) service site as a registered user. This allows the user to add a credit card,

billing address, and shipping address to their VSDB. The user may want to create VSDB information for test-purposes that does not have genuine and negotiable credit cards attached to it.

The VSDB server code may run a Luhn checksum test against all provided card numbers at input time. The Luhn checksum test is mainly intended as a convenience for users who may have mistyped their number, but it is not a credit card verification, security check, or authorization per se. The Luhn checksum test will prevent a purely random credit card number from being accepted as part of VirtualSAFE Deposit Box data. VirtualSAFE may performs other basic authorization and validation checks (e.g. state/ZIP code or Province/Postal code) when establishing a VSDB for a VirtualSAFE user. A phone number and e-mail addresses may be required fields for establishing a VSDB, even though they may be optional for a VirtualSAFE profile.

The VVP service is an easy-to-implement, server-based VSDB system that uses standard HTTP and Secure Sockets Layer (SSL) methods/PKI-based to post payment information to participant sites. VirtualSAFE supports the Electronic Commerce Modeling Language (ECML) which is an industry-standard e-commerce schema. The VSDB is compatible with popular web browsers. The VVP functions as follows:

1. When a user clicks an express purchase link at a participant site, the VVP service sends the user forward to the VirtualSAFE VSDB and then authenticates the user and presents a page showing a list of that user's credit cards and addresses. This information represents the user's VSDB. The user selects the means of payment and the address to use for the transaction and then presses a button to continue.

2. The VVP service then delivers the requested information from the user's VSDB to the participant site using a VVP order form returned over the SSL.

3. VirtualSAFE is responsible for authorizing the payment from the user. The participant site is then responsible for adding any gift options, and completing the optional fulfillment transaction.

4. If the user is a first-time VSDB user, the VVP service presents an empty form into which the user would enter the card and address he or she wants to use for the transaction. The user would then have to be authenticated prior to the purchase being approved, and the next time the user makes a purchase at a VirtualSAFE participant site, he or she would not need to retype any credit-card or address information as it will be already stored in VirtualSAFE and will automatically be passed on to the VSDB.

Policy issues related to VVP service and participant sites may include the following:

- Commitments and contractual obligations may be made when registering as a VirtualSAFE participant site.
- Requirements may be established regarding the display of VirtualSAFE links or images on participant sites.

Referring to FIGURES 30 and 31, the VVP service may also include a fund allocation feature which may be entitled "VirtualSAFE Trust and Allowance". This feature allows children and parents, or any authorized shared person, to relate to one another at a different level. Parents who are registered and authenticated users of VirtualSAFE may allocate a certain amount of pre-authorized spending money per month to their children on their credit/debit card. Similarly, businesses or friends who are registered and authenticated users of VirtualSAFE may allocate a certain amount of pre-authorized spending money from their accounts to authorized personnel, friends, etc. These values may be added, modified, and authorized at the beginning of each month. Consider the following example:

Parents/Businesses/Friends
Pre-authorized Payment/Transfer with Shared-Access
$450.00

Child's Name	Pre-authorized Amount Payment	Purchases	Balance
Robert Smith	150.00	100.00	50.00
Anna Smith	150.00	57.00	93.00
Billy Smith	150.00	148.00	2.00

Now consider the situation of business to business shared accounts in which two businesses operate with one another. According to agreement, this application allows one business to access the other business's account for a pre-authorized and predetermined amount. A lender opens an account or allows shared access to a borrower. Furthermore, this application allows financial transactions equivalent to the

commercially known line of credit, mortgage loan, or loan. Here, a borrower, as permitted by a shared access agreement, can debit a particular lender's account using the strong authentication provided by VirtualSAFE's Authentication Authority or, if necessary, by VirtualSAFE's predefined Attribute Authentication Authority. The pre-authorized user is able to both debit and credit the account as per agreement and policy. The same approach may be used for shared-access in a document environment, or application environment, in which one entity (i.e. the account holder) may allows another user access for sharing in accordance with user definitions and privileges.

Referring again to FIG. 24, further features of the VSDB will now be described.

Using a PKI-based secure application, an enrolling applicant is prompted to store personal information to the VirtualSAFE local or remote VirtualSAFE deposit box (VSDB). The depositing of information is a unique process. It involves encrypting the information with a PKI cryptographic scheme that uses a high-speed hybrid approach and then storing elements of it in a fragmented arrangement. Only the authenticated user can bring these pieces together again to render the information usable. In this process, the user profile becomes a virtual safety deposit box or part of a "virtual identity", the contents of which are accessible only to VirtualSAFE for the purpose of authentication, and only in the presence of the authorized user. The secure data is not accessible to any entity or application requesting user authentication or to VirtualSAFE administrators.

1. VirtualSAFE Deposit Box (VSDB) Functions

   - VSDB is a secured remote storage control with access control maintained by the Virtual Smart Card.

2. VirtualSAFE Deposit Box (VSDB) Usage

   - Single or multiple users can operate VSDB.

   - Users of VSDB will have different levels of privileges based on defined policy.

   - Users can communicate and store data in the following general formats: multi-lingual, multi-calendar, multi-currency, and multi-format (i.e. documents, drawings, formulas, and other file formats).

3. VirtualSAFE Deposit Box (VSDB) Types. VSDB supports the following Deposit Box formats:

   - Private (i.e. Private and Family related information and Third Party authentication mechanisms, PINs, etc.)

   - Financial (i.e. All Private Financial related and Business/Government Financial related data.)

   - Business (i.e. All Business related data – Business Numbers, Documents, Legal and/or HR Documents, Drawings, etc.)

- Government (i.e. All Government related data – Business Numbers, Documents, Legal and/or HR Documents, Drawings, etc.)

- General (May be local or remote for customer based on Policy.)

- Transaction (May be local or remote and this type of VSDB supports all data related to all transactions maintained by VirtualSAFE – All Private information is encrypted and maintained as per Privacy Policy and Government regulations.)

POS-VSC Emulation. Referring to FIG. 25, there is shown a block diagram of the point-of-sale (POS) and virtual smart card (VSC) emulation process in VirtualSAFE. POS-VSC emulation is a low cost replacement for the physical smart card application. POS-VSC may be easily implemented on an existing financial network. Using the Virtual Smart Card (VSC) reduces the high cost of physical smart card implementation and critical maintenance issues. VirtualSAFE's PKI structure is used to authenticate users on any POS premise based on individual PINs (Personal Identification Numbers) in accordance with selected European standards. The Point of Sale (POS)/Virtual Smart Card emulation process may be performed as follows:

1. Magnetic Card

   - User uses Credit/Debit card.

2. Point Of Sale (POS)

   - POS requests Credit/Debit card payment authorization.

3. Smart Card Reader

- Merchant Smart Card identifies merchant to VirtualSAFE.
- Received message from POS sent to VirtualSAFE.

4. Transaction Request

- VirtualSAFE receives transaction request.
- VirtualSAFE requests user PIN for authentication purposes.

5. User Authentication Pin

- User enters PIN for authentication purposes.
- Smart Card reader sends encrypted data to VirtualSAFE.

6. Authentication

- VirtualSAFE process authenticates customer.

7. Messaging

- Payment requested from the bank.

8. Payment Processing

- Credit/Debit card payment authorized/settled.

9. Transaction Log

- Message sent to VirtualSAFE.

- All transaction steps are recorded.

10. Smart Card Reader Confirmation

- Smart Card reader receives authorization from Credit card processing department.

- Decrypted message is sent to POS.

11. Point Of Sale Authorization

- POS receives authorized message in standard format.

- Transaction authorized and printed.

ATM-VSC Emulation. Referring to FIG. 26, there is shown a block diagram of the ATM and virtual smart card (VSC) emulation process in VirtualSAFE. ATM-VSC Emulation provides a solutions for physical smart card applications implemented on existing networks. Using a Virtual Smart Card (VSC) reduces the high cost of physical smart card implementation and critical maintenance issues. The user authentication process is based on VirtualSAFE's PKI structure. VirtualSAFE applications implemented on supported servers does not require significant changes to existing ATM applications and networks. A security layer is implemented in existing applications and financial networks in accordance with current standards. The ATM/Virtual Smart Card emulation process may be performed as follows:

1. Magnetic Card

- User uses Credit/Debit magnetic card.

2. Automatic Teller Machine (ATM)

- The ATM requests Credit/Debit transaction authorization.

3. Add-On ATM Application

- Add-on ATM application maintains digital certificate with all security functions.
- Magnetic reader reads card hash information.
- Digital certificate encrypts and signs transaction and private information.

4. Transaction Request

- VirtualSAFE received transaction request.
- VirtualSAFE requests User PIN for authentication purposes.

5. User Authentication PIN

- User enters PIN for authentication purposes.
- ATM sends encrypted data to VirtualSAFE.

6. Authentication

- VirtualSAFE process authenticates customer.

7. Messaging

- Payment requested from the bank.

8. Payment Processing

- Credit/Debit card payment authorized/settled.

9. Transaction Log

- Message sent to VirtualSAFE.
- All transaction steps are recorded.

10. ATM Confirmation

- ATM receives authorization message from Credit Card processing department.

11. ATM Authorization

- Transaction authorized and printed.

POS/ATM/Wireless. Referring to FIG. 27, there is shown a block diagram of the wireless POS and ATM process in VirtualSAFE. With respect to wireless VirtualSAFE access, the user may access the VirtualSAFE application through an analog or a digital wireless network using one of the following devices: cellular phone, PDA, two way radio, satellite, etc. VirtualSAFE provides a secure wireless application both locally and via the server. To wirelessly communicate with

VirtualSAFE, either a standard wireless network can be used or a local wireless network (i.e. Blackberry, Blue Tooth, Infrared, etc.) may be used. With respect to local wireless VirtualSAFE access, the user may access the VirtualSAFE wireless application either locally or remotely. The local wireless application may communicate to a remote device through a conventional or wireless network. The local wireless authentication application may communicate to a remote VirtualSAFE device through a conventional or wireless network.

SAFEcheck. Referring to FIG. 28, there is shown a block diagram of the SAFEcheck process in VirtualSAFE. The VirtualSAFE Check Processing (VCP) enables streamlined and secure check processing and payments through a remote network connection. The VirtualSAFE method and system is employed in a traditional check processing protocol in which VirtualSAFE authenticates a check clearing transaction. This capability allows for the integration of electronic payments and check processing. The SAFEcheck process may be performed as follows:

1. User Browses The Merchant Site

2. User Selects SAFEcheck Payment

    - A digitally signed shopping cart contents and payment amounts are sent to VirtualSAFE.

    - User is then redirected to the VirtualSAFE secured site for further authentication.

3. User Authentication

- VirtualSAFE defines authentication level depending on payment amount and SAFEcheck Policy.

4. Account Selected

- User selects appropriate checking account from availability list.

5. Account Digital Signature (DS)

- User digitally signs SAFEcheck.
- SAFEcheck signed with web certificate.
- SAFEcheck signed with VirtualSAFE certificate.

6. Clearance Request

- VirtualSAFE issues clearance request.

7. Financial Institution

- Receives SAFEcheck for check presentment.

8. Check Printer

- SAFEcheck has been printed on premises including customer signature.
- Printer uses regulated check paper with appropriate coding.

9. Electronic Check Presentment (ECP)

- VirtualSAFE application interfaces with Electronic Check Presentment module.
- SAFEcheck cleared and processed.

10. Confirmation

- VirtualSAFE receives confirmation.
- VirtualSAFE sends confirmation to merchant and user to complete transaction.

11. Merchant Prints SAFEcheck

- Merchant prints out user signed copy of cleared check.
- User optionally signs SAFEcheck at merchant premises.

Physical Access Control. Referring to FIG. 29, there is shown a block diagram of physical access control in VirtualSAFE. Physical Access Control or SAFEpac refers to the storage in VirtualSAFE of secure entry information. With respect to employee/visitor door access, at least three scenarios may be supported as follows:

1. Local Physical Access

- Local office user access requested.

- Request is processed locally.

2. Remote Physical Access

- Remote office user access requested.
- Request is processed remotely.

3. VirtualSAFE Controlled High Security Access

- Remote office user access requested.
- Request is processed remotely.

Multiple entry levels may also be supported as follows:

1. Entry Level 1

- Building user requests access to local branch.
- Building control unit validates Digital Certificate access level and authorizes access.

2. Entry Level 2

- Building user requests access to building Secured room.
- Building Control Unit validates Digital Certificate access level and requests User PIN.

3. Entry Level 3

- Building user requests access to building High-Secured room.
- Building Control Unit forwards validation of the Digital Certificate from Security Company Controller.
- User must provide PIN.

4. Entry Level 4

- Building user requests access to building Restricted Area.
- Building Control Unit forwards validation of the Digital Certificate from VirtualSAFE through Security Company.
- User must provide VirtualSAFE PIN.

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A transaction server for performing a transaction over a network using a virtual smart card said server comprising:
    a) a virtual smart card database having a plurality of records each record including a virtual card identification and a value corresponding to a single virtual smart card;
    b) a security module;
    c) an emulator for emulating a smart card, said emulator for receiving smart card commands and processing said commands in conjunction with said virtual smart card database and said security module; and
    d) a virtual card reader module for receiving said smart card commands and relaying said commands to said smart card emulator whereby transactions are performed over said network using one or more said records and said virtual smart card database.

2. A method for performing a transaction over a network using a virtual smart card and a server, said method comprising the steps of:
    a) creating a plurality of records on a virtual smart card database, each record including a virtual card identifier and a value corresponding to a single virtual smart card;
    b) receiving smart card commands via a smart card emulator and processing said commands in conjunction with said virtual smart card database and a security module; and
    c) receiving said smart card commands via a virtual card reader module and relaying said commands to said smart card emulator whereby transactions are performed over said network using said server and one or more of said records in said virtual smart card database.

3. A server as defined in claim 1, said security module including a plurality of encryption algorithms.

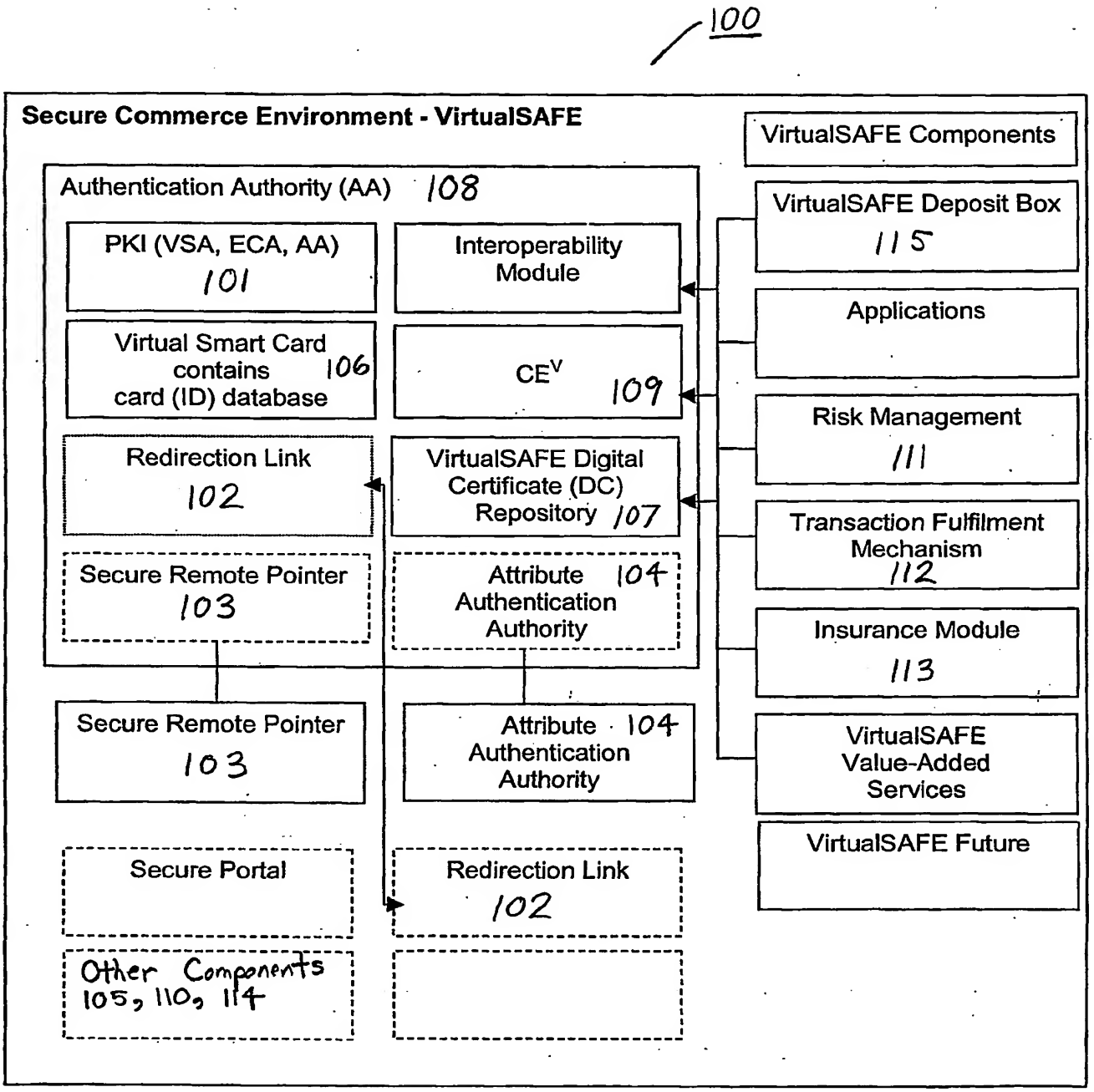


FIG. 1

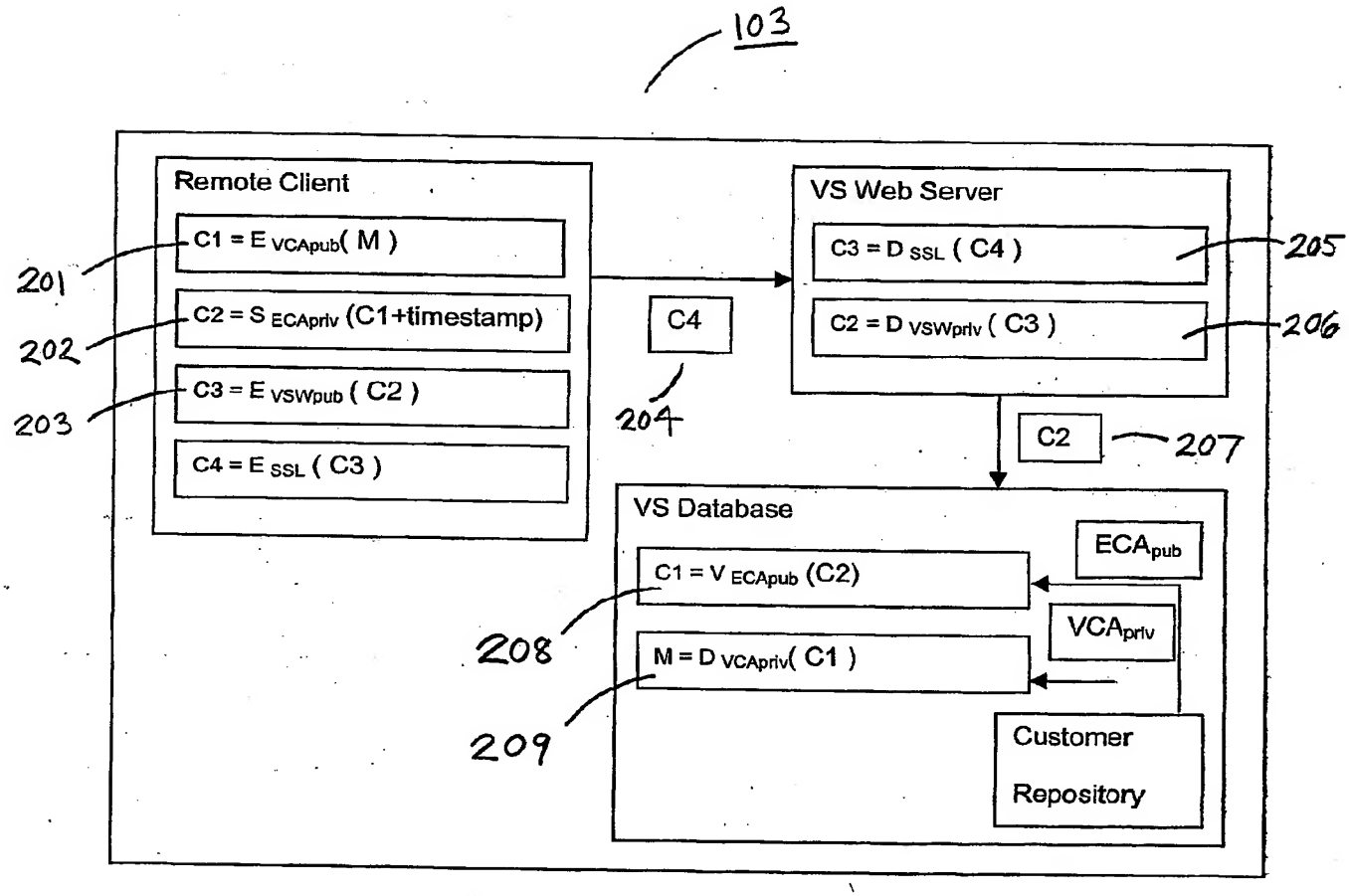


FIG. 2

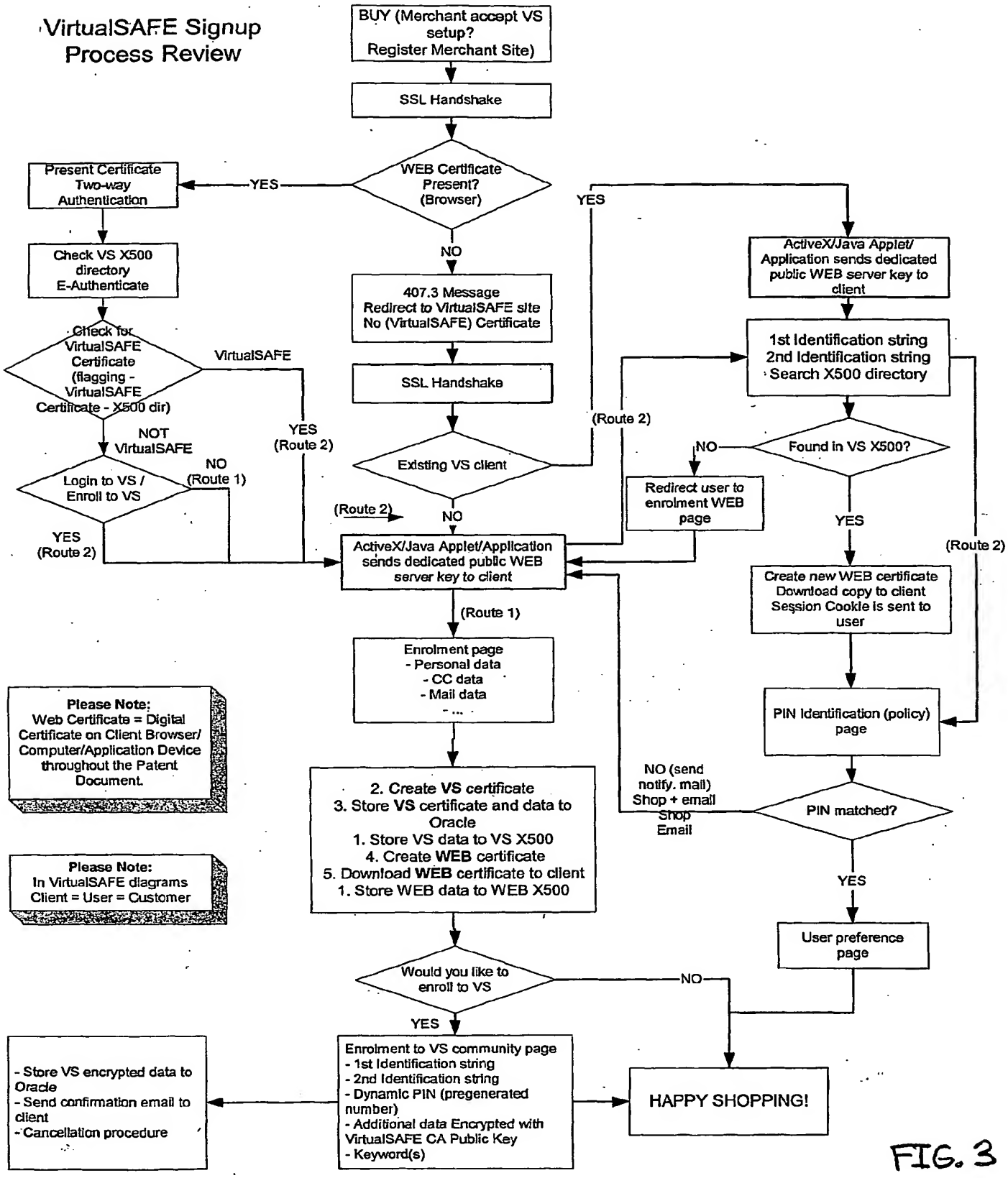

VirtualSAFE Signup Process Review
BUY (Merchant accept VS setup? Register Merchant Site)
SSL Handshake
WEB Certificate Present? (Browser)
YES
Present Certificate Two-way Authentication
Check VS X500 directory E-Authenticate
Check for VirtualSAFE Certificate (flagging - VirtualSAFE Certificate - X500 dir)
VirtualSAFE
YES (Route 2)
NOT VirtualSAFE
Login to VS / Enroll to VS
NO (Route 1)
YES (Route 2)
NO
407.3 Message Redirect to VirtualSAFE site No (VirtualSAFE) Certificate
SSL Handshake
Existing VS client
(Route 2)
NO
ActiveX/Java Applet/Application sends dedicated public WEB server key to client
(Route 1)
Enrolment page
- Personal data
- CC data
- Mail data
- ...
2. Create VS certificate
3. Store VS certificate and data to Oracle
1. Store VS data to VS X500
4. Create WEB certificate
5. Download WEB certificate to client
1. Store WEB data to WEB X500
Would you like to enroll to VS
YES
NO
Enrolment to VS community page
- 1st Identification string
- 2nd Identification string
- Dynamic PIN (pregenerated number)
- Additional data Encrypted with VirtualSAFE CA Public Key
- Keyword(s)
- Store VS encrypted data to Oracle
- Send confirmation email to client
- Cancellation procedure
HAPPY SHOPPING!
YES
ActiveX/Java Applet/ Application sends dedicated public WEB server key to client
1st Identification string
2nd Identification string
Search X500 directory
Found in VS X500?
NO
Redirect user to enrolment WEB page
YES
Create new WEB certificate
Download copy to client
Session Cookie is sent to user
PIN Identification (policy) page
PIN matched?
NO (send notify. mail) Shop + email Shop Email
YES
User preference page
(Route 2)
Please Note:
Web Certificate = Digital Certificate on Client Browser/ Computer/Application Device throughout the Patent Document.
Please Note:
In VirtualSAFE diagrams Client = User = Customer

FIG. 3

VirtualSAFE Sign-up Process

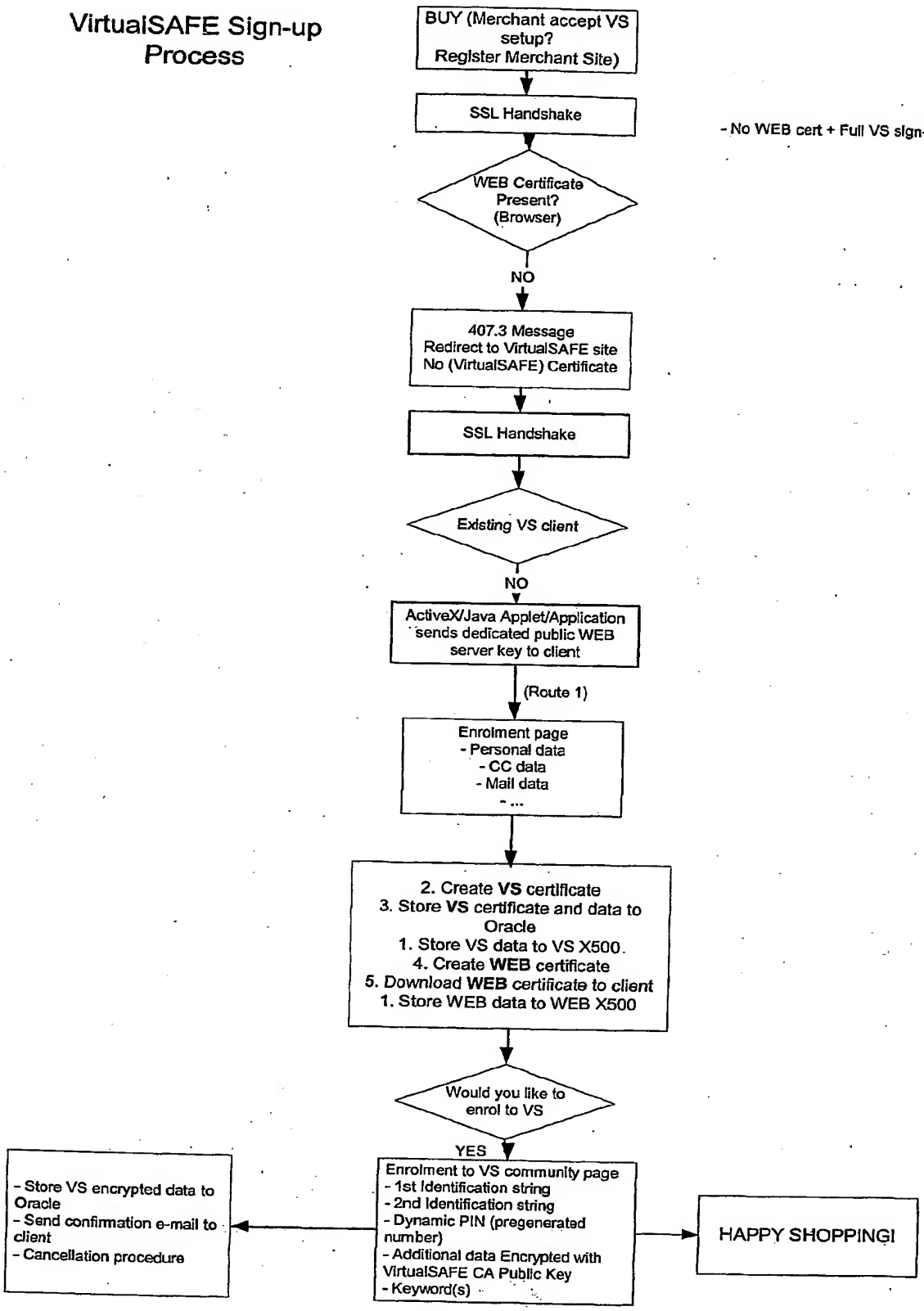


FIG. 4

VirtualSAFE Signup Process

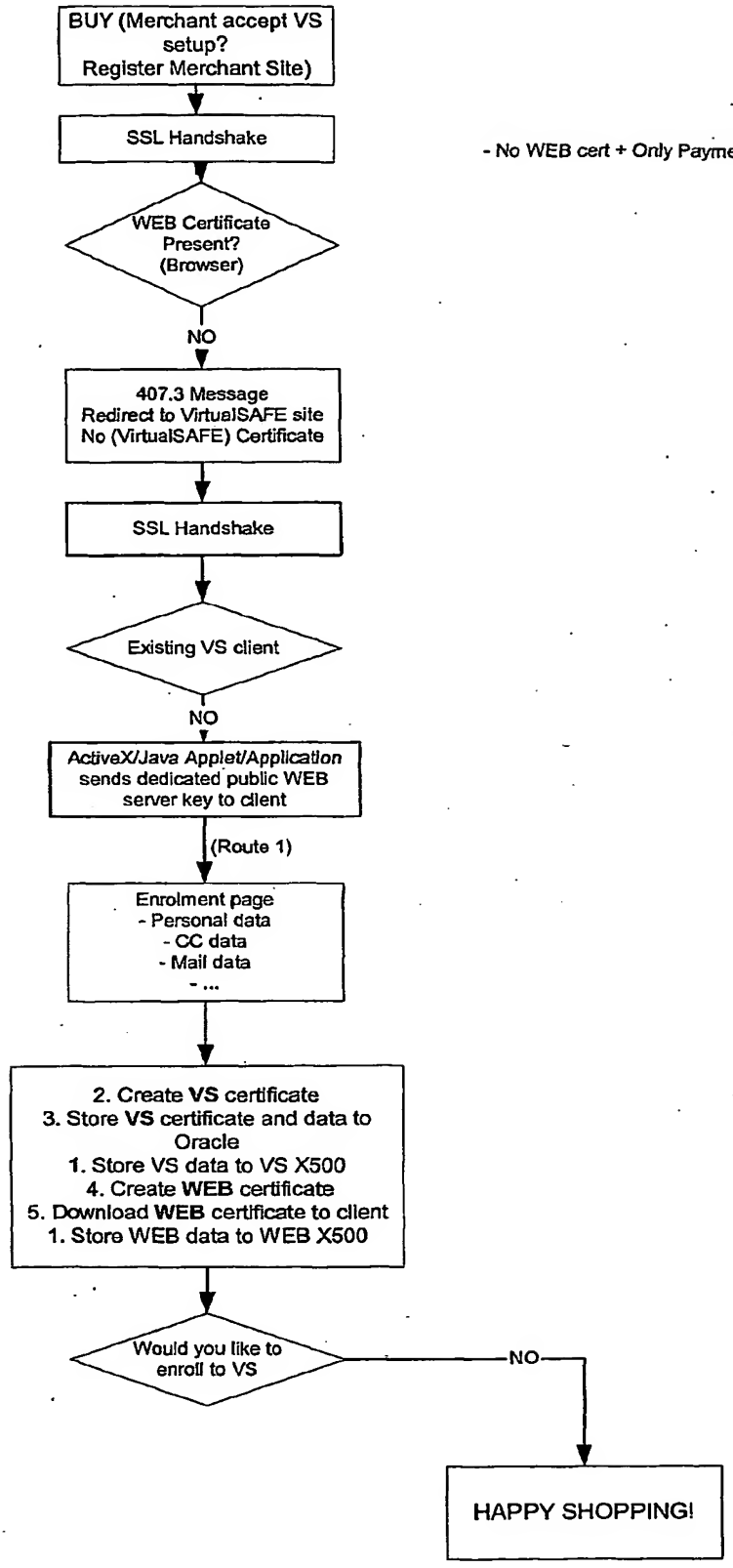


FIG. 5

VirtualSAFE Signup Process

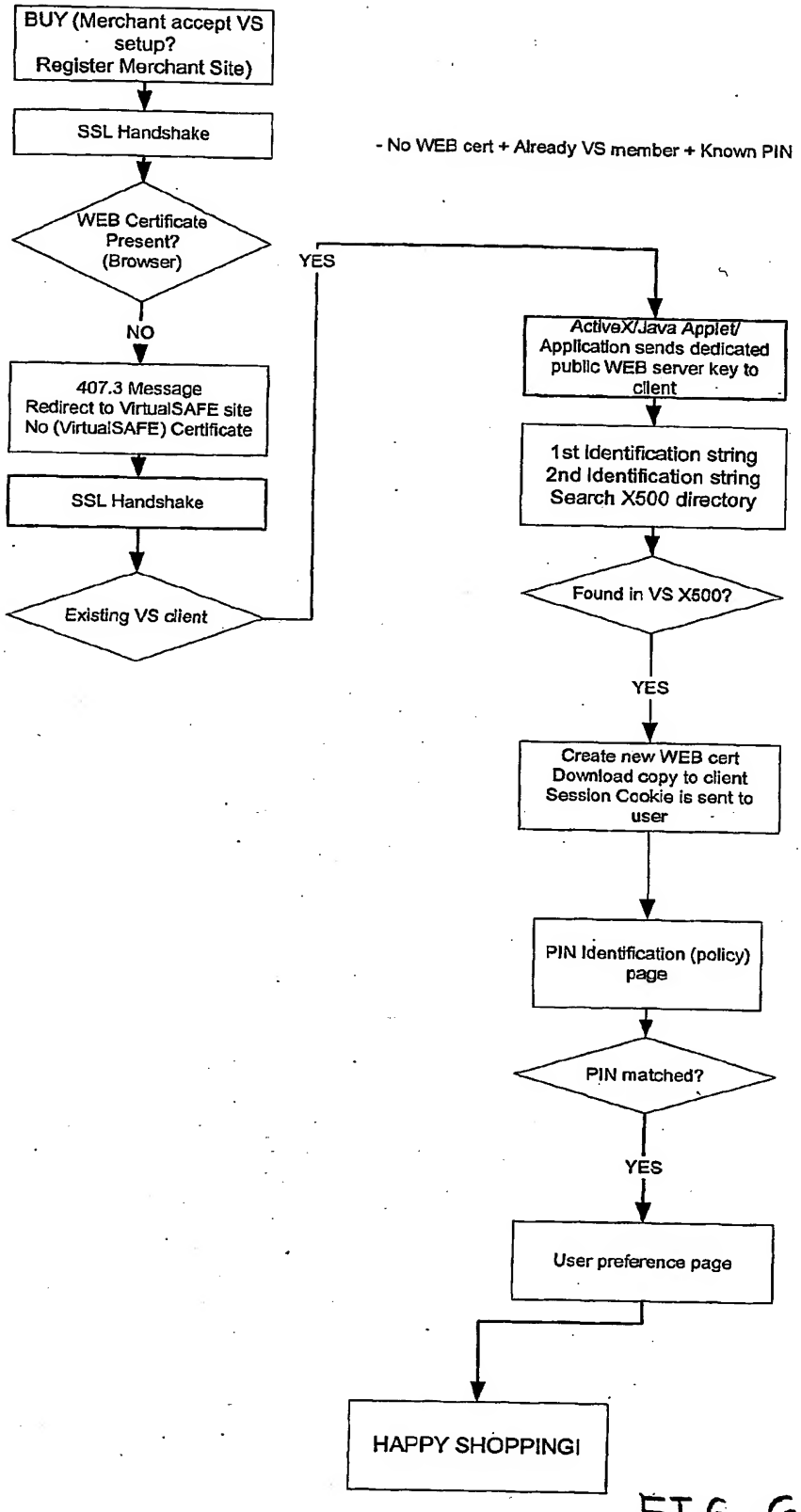


FIG. 6

VirtualSAFE Signup Process

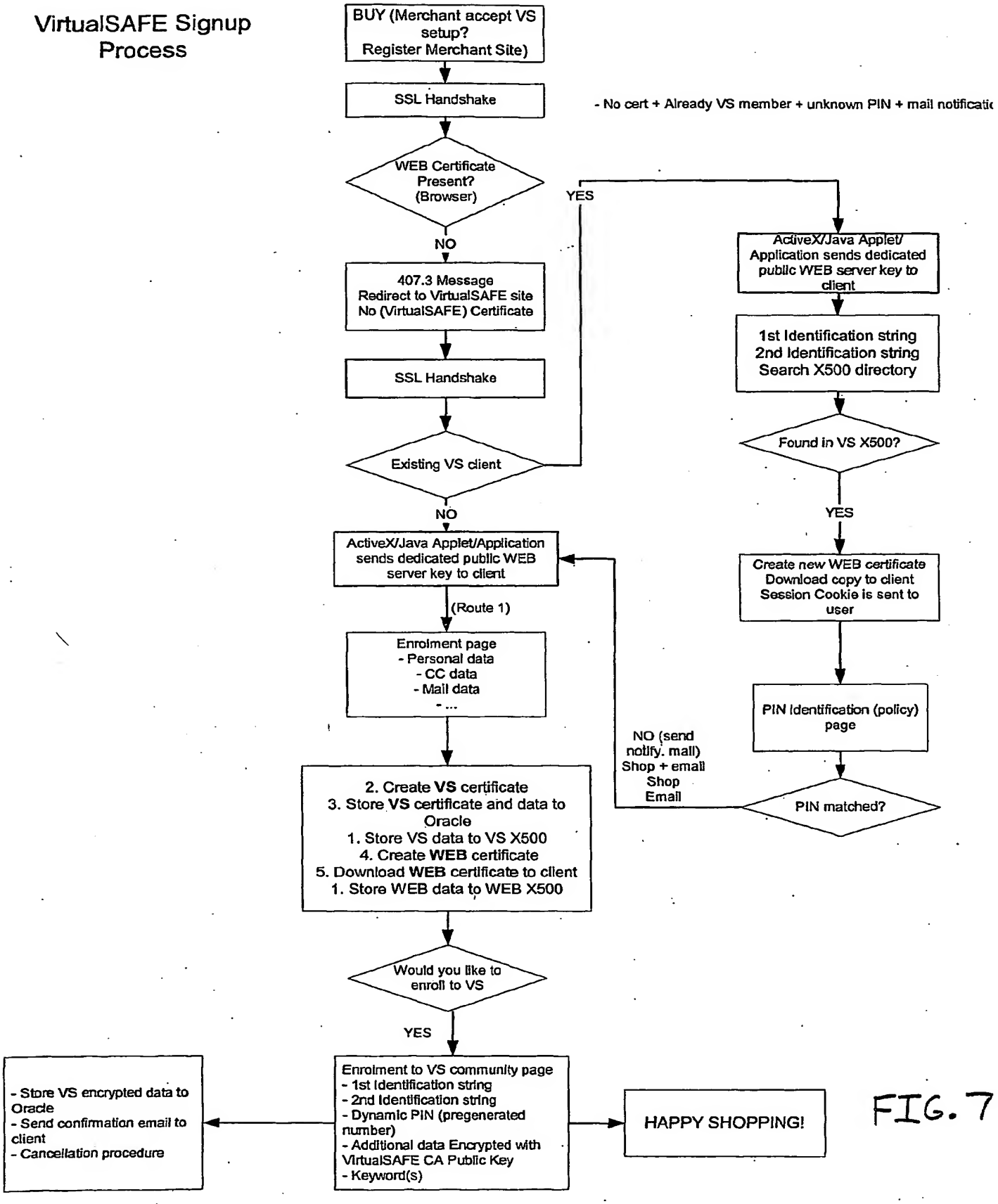


FIG. 7

VirtualSAFE Signup Process

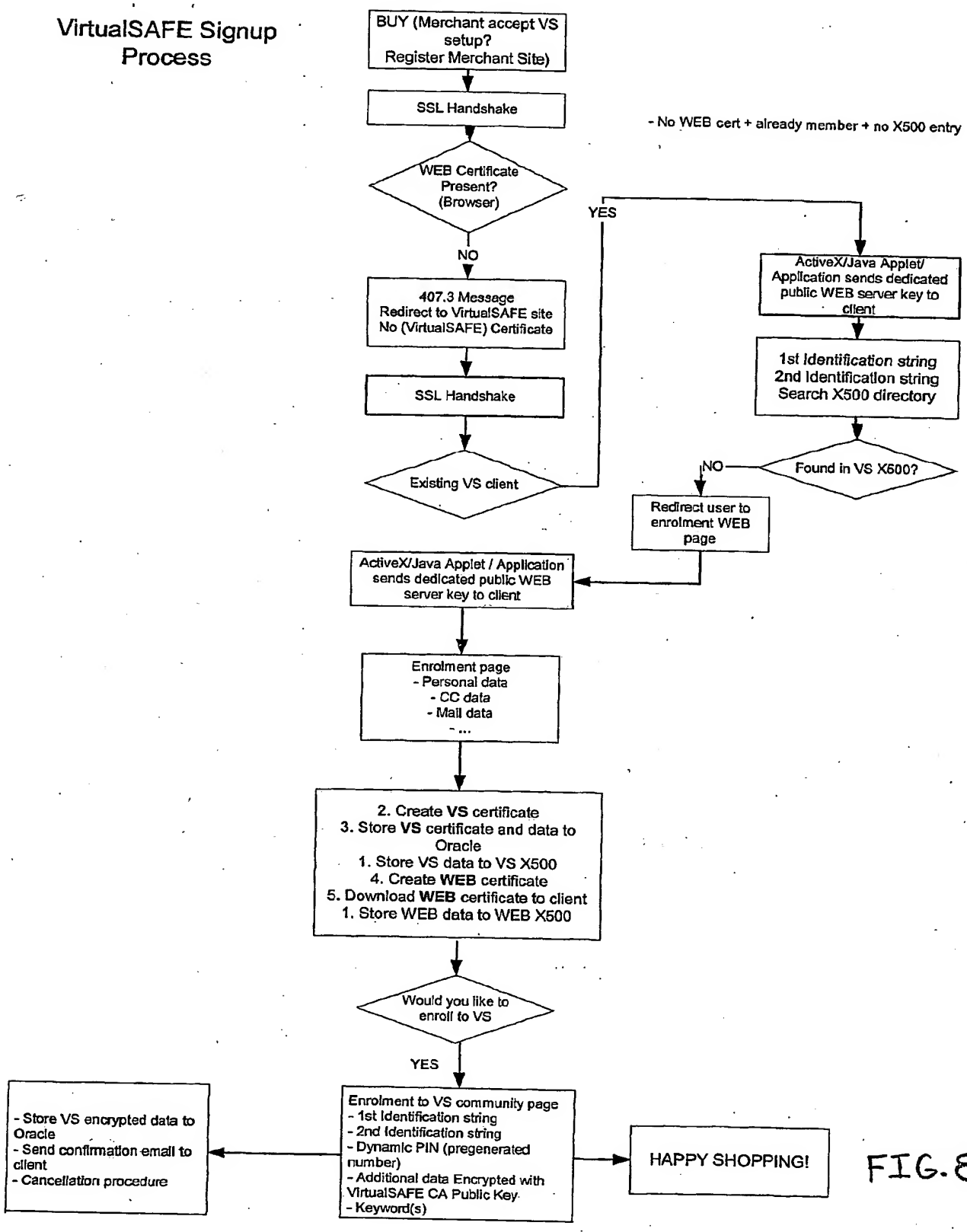


FIG. 8

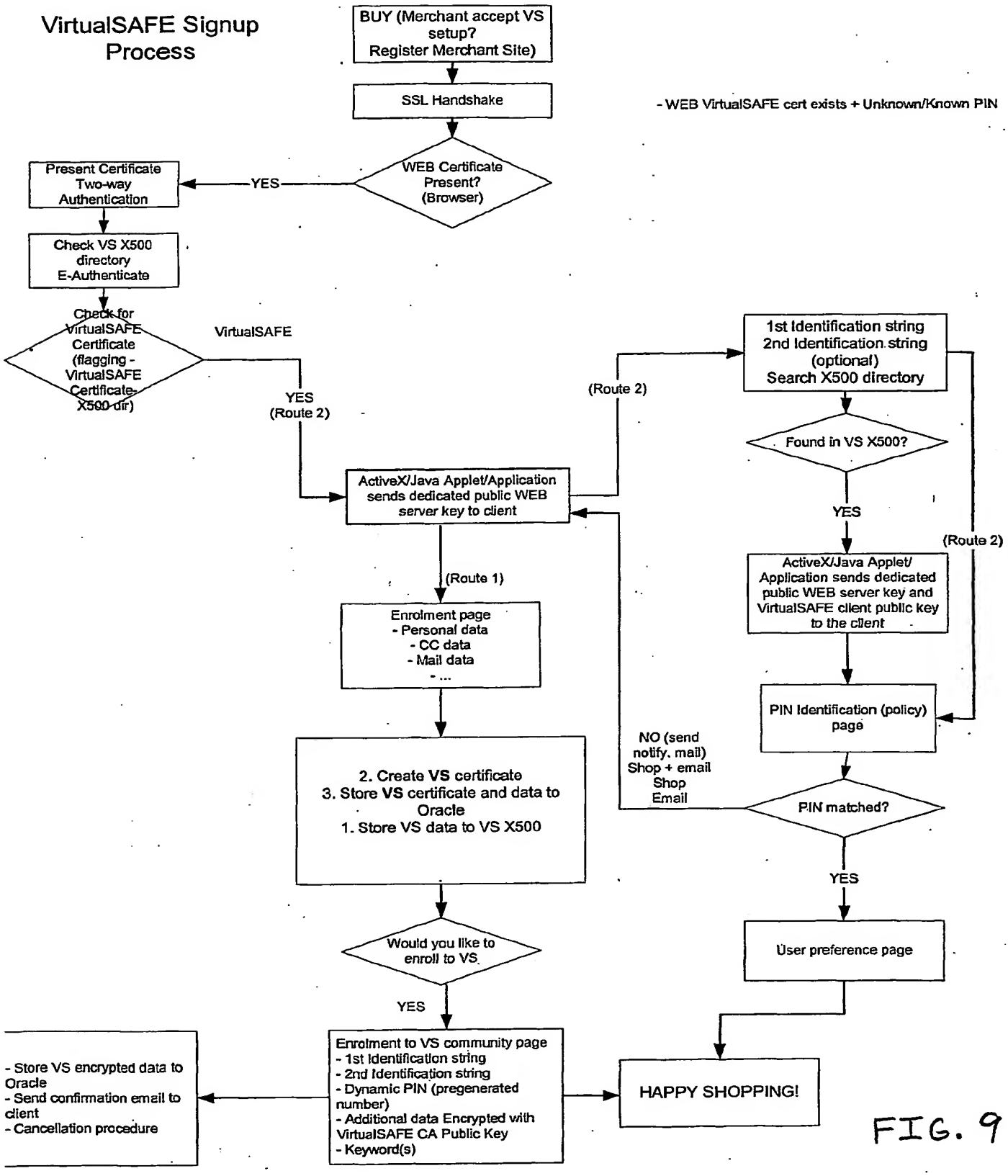
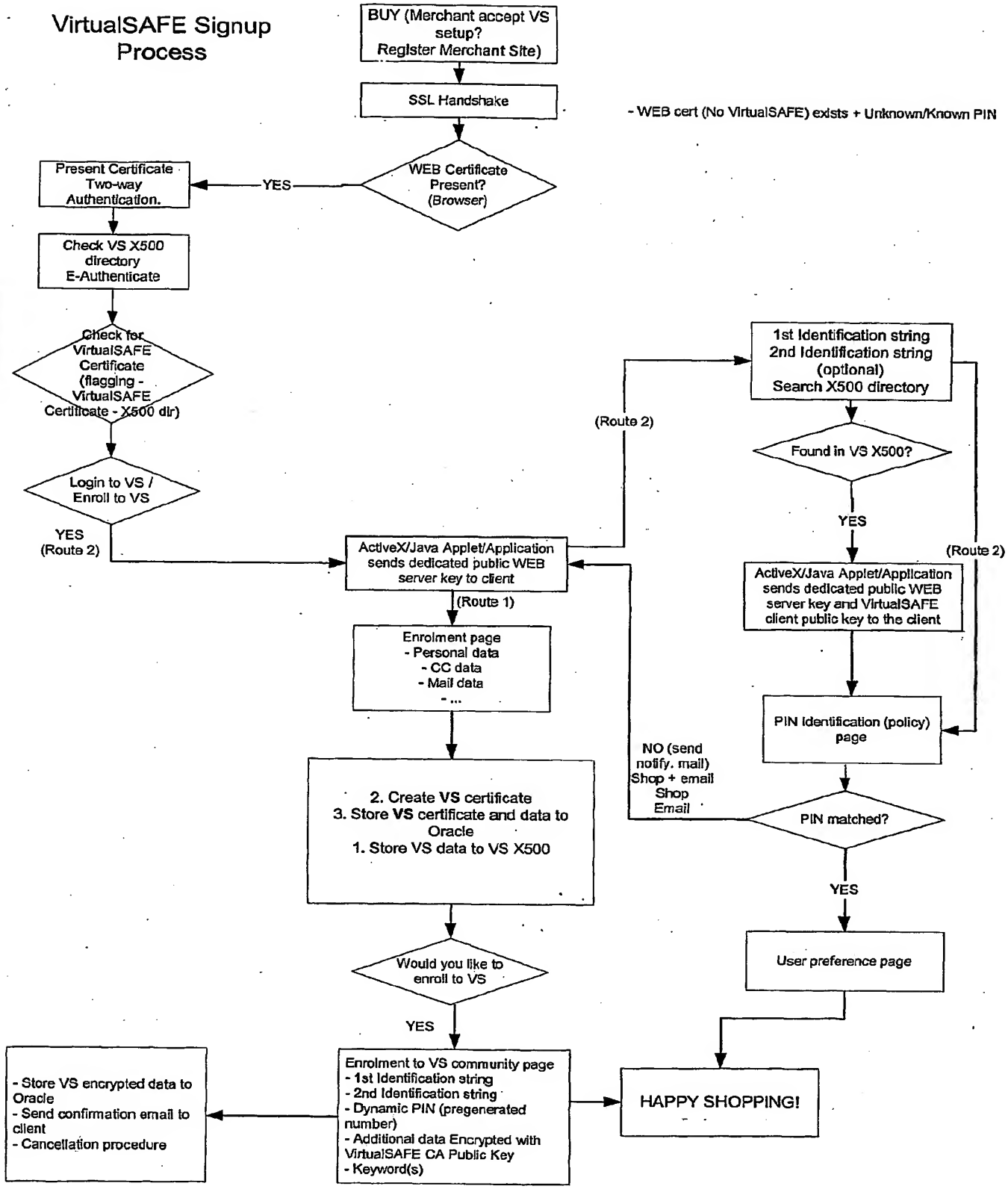

VirtualSAFE Signup Process
BUY (Merchant accept VS setup? Register Merchant Site)
SSL Handshake
WEB Certificate Present? (Browser)
YES
Present Certificate Two-way Authentication
Check VS X500 directory E-Authenticate
Check for VirtualSAFE Certificate (flagging - VirtualSAFE Certificate-X500-dir)
VirtualSAFE
YES (Route 2)
- WEB VirtualSAFE cert exists + Unknown/Known PIN
1st Identification string
2nd Identification string (optional)
Search X500 directory
(Route 2)
Found in VS X500?
YES
(Route 2)
ActiveX/Java Applet/Application sends dedicated public WEB server key to client
ActiveX/Java Applet/ Application sends dedicated public WEB server key and VirtualSAFE client public key to the client
(Route 1)
Enrolment page
- Personal data
- CC data
- Mail data
- ...
PIN Identification (policy) page
NO (send notify. mail) Shop + email Shop Email
2. Create VS certificate
3. Store VS certificate and data to Oracle
1. Store VS data to VS X500
PIN matched?
YES
Would you like to enroll to VS.
User preference page
YES
- Store VS encrypted data to Oracle
- Send confirmation email to client
- Cancellation procedure
Enrolment to VS community page
- 1st Identification string
- 2nd Identification string
- Dynamic PIN (pregenerated number)
- Additional data Encrypted with VirtualSAFE CA Public Key
- Keyword(s)
HAPPY SHOPPING!

FIG. 9


VirtualSAFE Signup Process
BUY (Merchant accept VS setup? Register Merchant Site)
SSL Handshake
WEB Certificate Present? (Browser)
YES
Present Certificate Two-way Authentication.
Check VS X500 directory E-Authenticate
Check for VirtualSAFE Certificate (flagging - VirtualSAFE Certificate - X500 dir)
Login to VS / Enroll to VS
YES (Route 2)
- WEB cert (No VirtualSAFE) exists + Unknown/Known PIN
1st Identification string
2nd Identification string (optional)
Search X500 directory
Found in VS X500?
YES
(Route 2)
(Route 2)
ActiveX/Java Applet/Application sends dedicated public WEB server key to client
(Route 1)
ActiveX/Java Applet/Application sends dedicated public WEB server key and VirtualSAFE client public key to the client
Enrolment page
- Personal data
- CC data
- Mail data
- ...
PIN Identification (policy) page
NO (send notify. mail) Shop + email Shop Email
PIN matched?
YES
2. Create VS certificate
3. Store VS certificate and data to Oracle
1. Store VS data to VS X500
User preference page
Would you like to enroll to VS
YES
Enrolment to VS community page
- 1st Identification string
- 2nd Identification string
- Dynamic PIN (pregenerated number)
- Additional data Encrypted with VirtualSAFE CA Public Key
- Keyword(s)
HAPPY SHOPPING!
- Store VS encrypted data to Oracle
- Send confirmation email to client
- Cancellation procedure

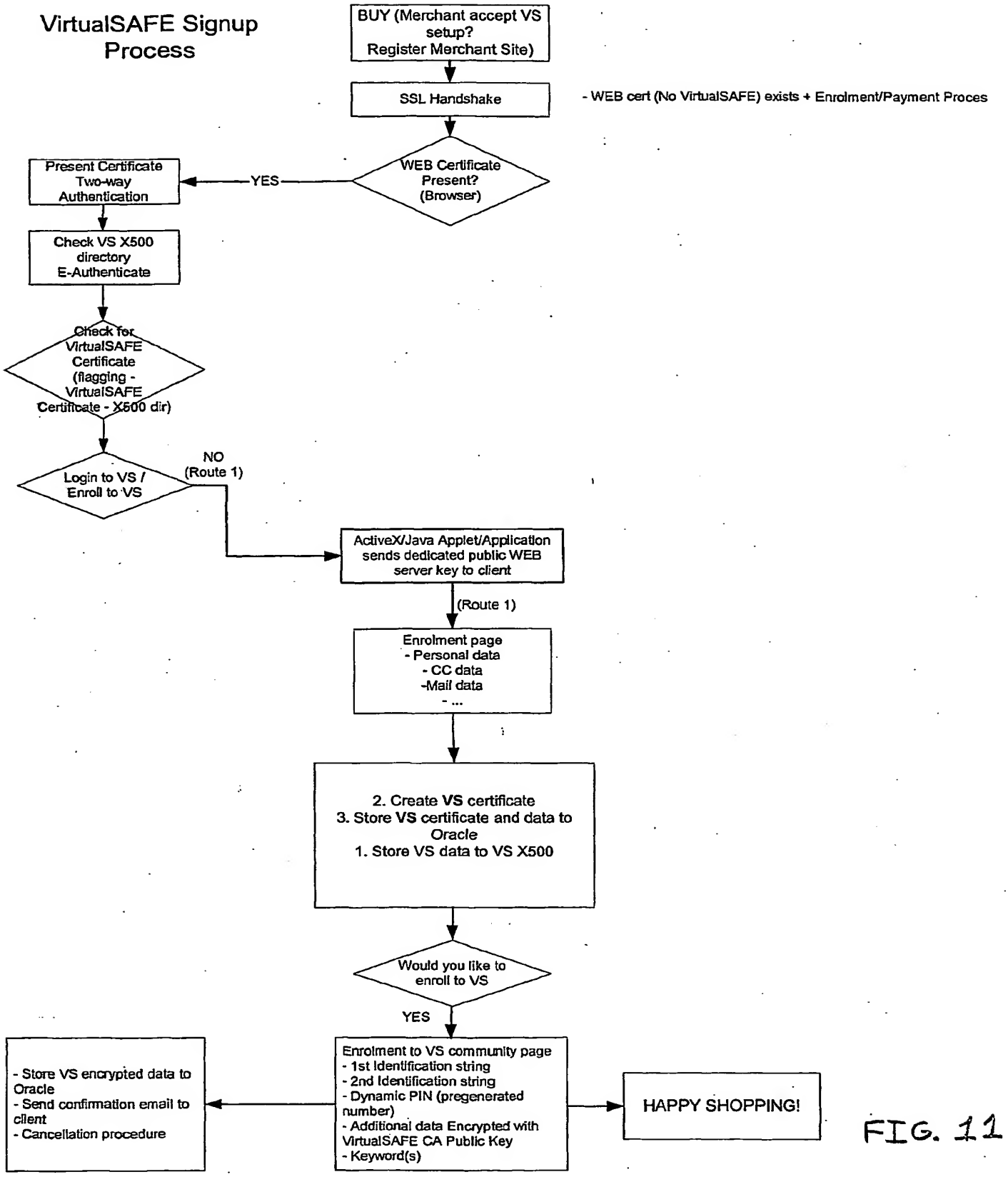

VirtualSAFE Signup Process
BUY (Merchant accept VS setup? Register Merchant Site)
SSL Handshake
- WEB cert (No VirtualSAFE) exists + Enrolment/Payment Proces
WEB Certificate Present? (Browser)
YES
Present Certificate Two-way Authentication
Check VS X500 directory E-Authenticate
Check for VirtualSAFE Certificate (flagging - VirtualSAFE Certificate - X500 dir)
Login to VS / Enroll to VS
NO (Route 1)
ActiveX/Java Applet/Application sends dedicated public WEB server key to client
(Route 1)
Enrolment page
- Personal data
- CC data
-Mail data
- ...
2. Create VS certificate
3. Store VS certificate and data to Oracle
1. Store VS data to VS X500
Would you like to enroll to VS
YES
Enrolment to VS community page
- 1st Identification string
- 2nd Identification string
- Dynamic PIN (pregenerated number)
- Additional data Encrypted with VirtualSAFE CA Public Key
- Keyword(s)
- Store VS encrypted data to Oracle
- Send confirmation email to client
- Cancellation procedure
HAPPY SHOPPING!

FIG. 11

VirtualSAFE
CA Processes
(Partial)

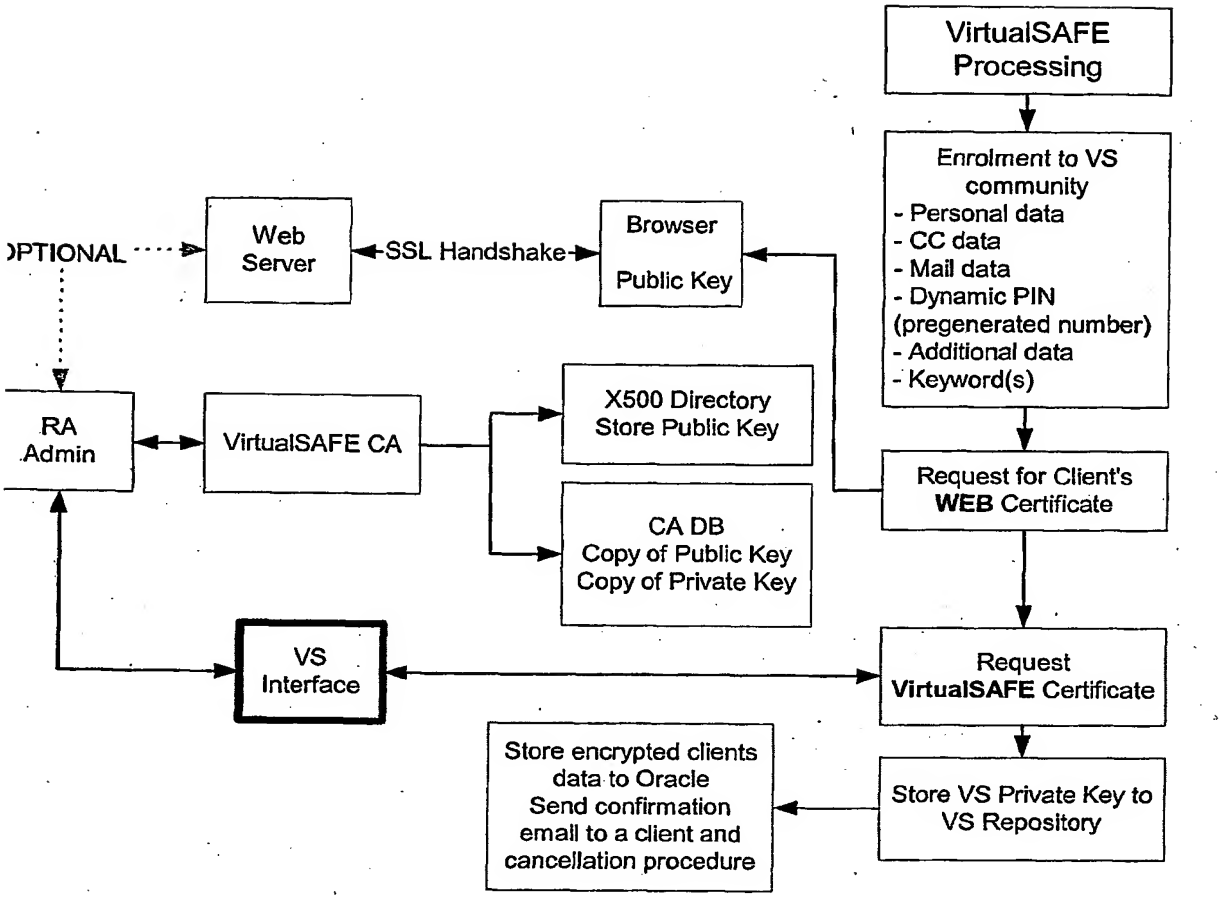
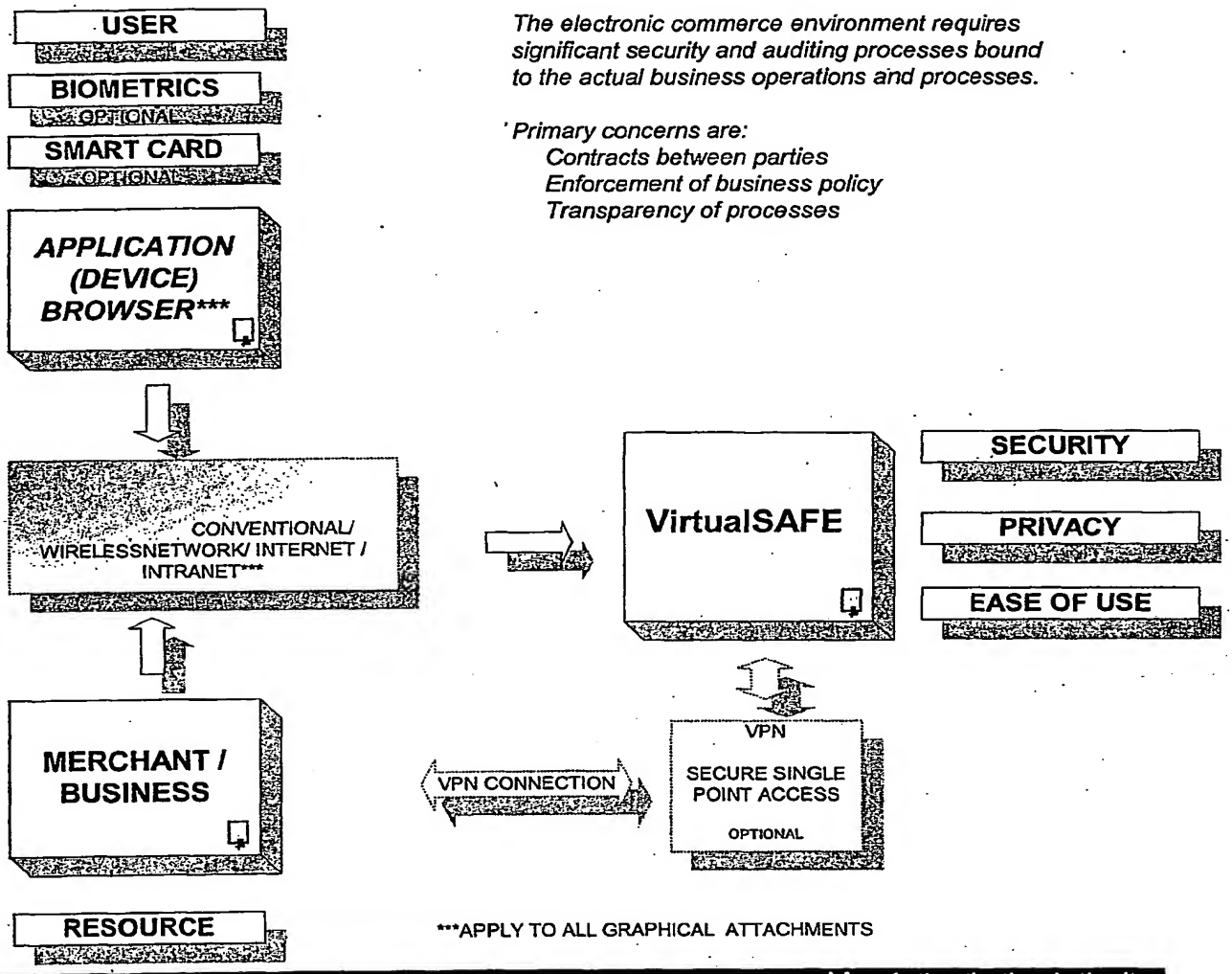


FIG. 12

Participants



The electronic commerce environment requires significant security and auditing processes bound to the actual business operations and processes.

Primary concerns are:
- *Contracts between parties*
- *Enforcement of business policy*
- *Transparency of processes*

CONTRACTUAL RELATIONSHIP BETWEEN PARTIES

1 - VirtualSAFE BUSINESS POLICY

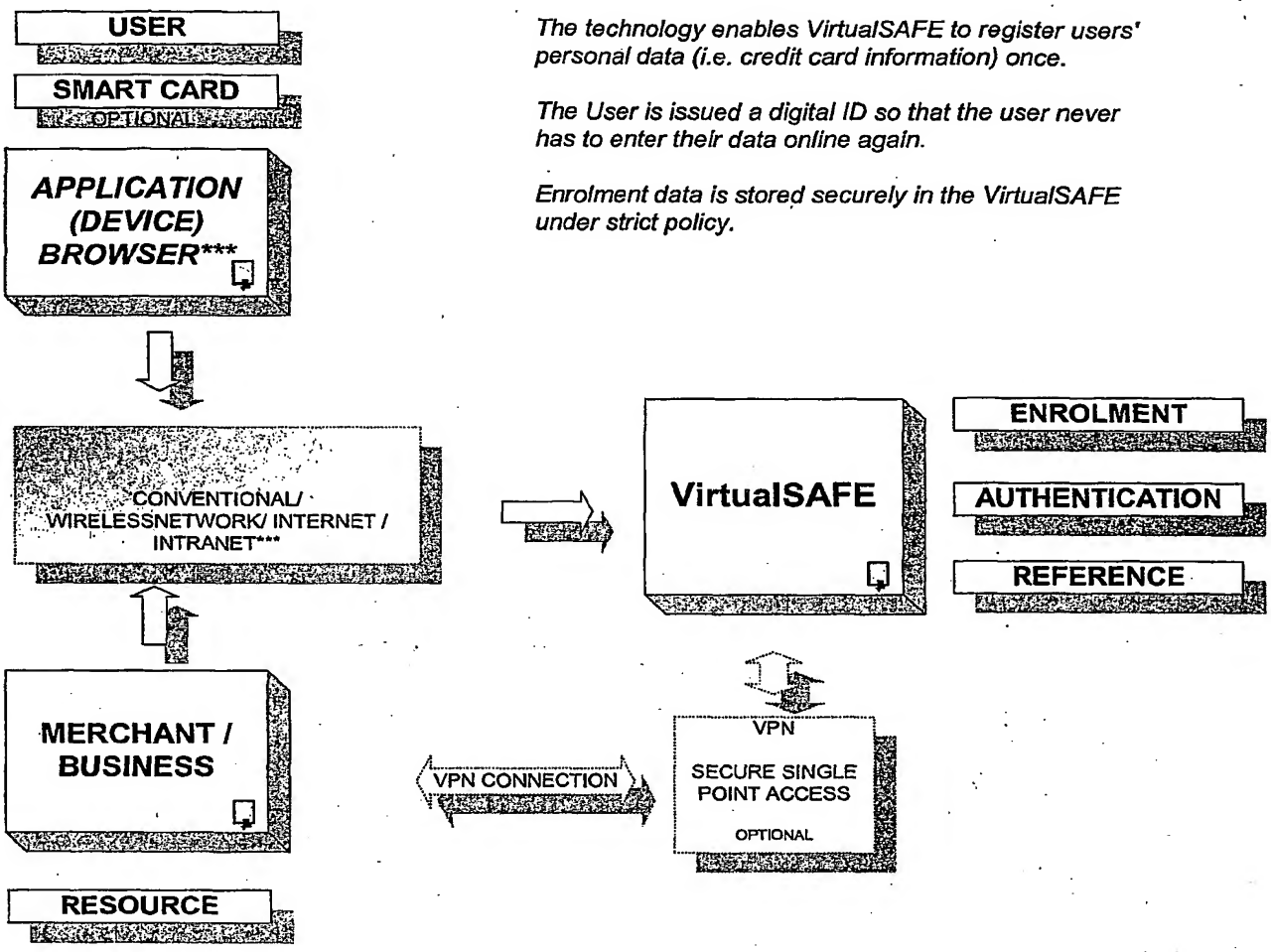
- **PRIVACY**
  - ***ONLY USER HAS ACCESS TO THEIR PRIVATE INFORMATION***
  - EU COMPLIANT PRIVACY REGULATION
  - NORTH AMERICAN COMPLIANT PRIVACY REGULATION
  - THIRD PARTY ACCESS REGULATED ONLY BY COURT ORDER
- **SECURITY**
  - 140 FIPS/3 COMPLIANT
  - 7/24 MONITORING
  - REMOTE VIRUS SCAN
- **EASE OF USE**
  - VirtualSAFE DOES NOT CHANGE PRESENT USER EXPERIENCE
  - ***PRIVATE INFORMATION ENTERED INTO VirtualSAFE ONLY ONCE***
  - VirtualSAFE USER EXPERIENCE **"CLICK-AND-GO"** FROM ANY SITE

2 - BUSINESS POLICY

- **VirtualSAFE COMPLIES TO BUSINESS POLICY**

FIG. 13

Enrolment



The technology enables VirtualSAFE to register users' personal data (i.e. credit card information) once.

The User is issued a digital ID so that the user never has to enter their data online again.

Enrolment data is stored securely in the VirtualSAFE under strict policy.

VirtualSAFE ENROLMENT

1 - ENROLMENT TO VirtualSAFE

- RESOURCE ENROLMENT
- CUSTOMER ENROLMENT
- ATTRIBUTE RESOURCE ENROLMENT
- EMPLOYEE ENROLMENT
  - IT ACCESS CONTROL
  - PHYSICAL ACCESS CONTROL (LOCAL AND REMOTE)

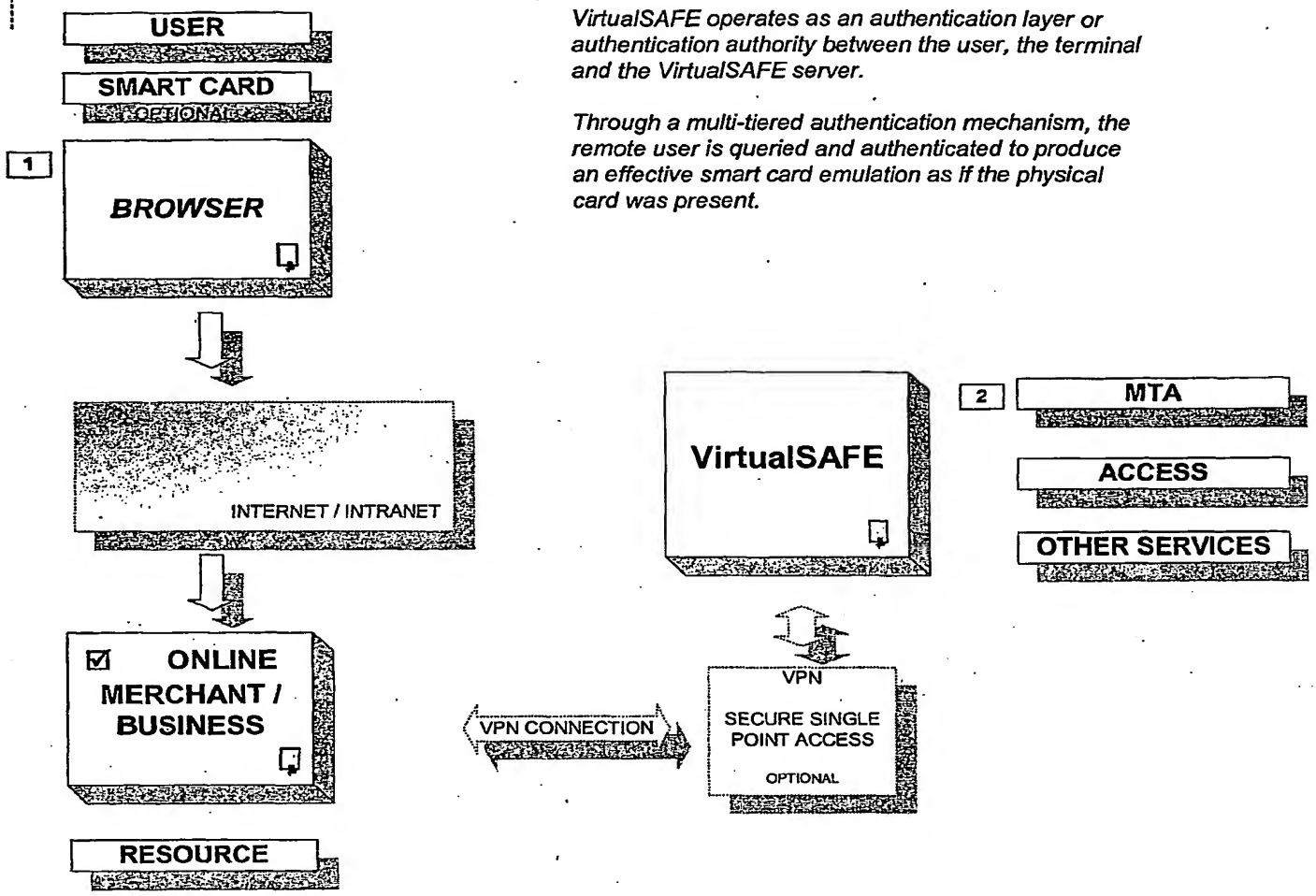
2 - VirtualSAFE CUSTOMER AUTHENTICATION ENROLMENT

3 - USER AUTHENTICATION

4 - REFERENCE VALIDATION

FIG. 14

Online Transactions



VirtualSAFE operates as an authentication layer or authentication authority between the user, the terminal and the VirtualSAFE server.

Through a multi-tiered authentication mechanism, the remote user is queried and authenticated to produce an effective smart card emulation as if the physical card was present.

AA - Authentication Authority

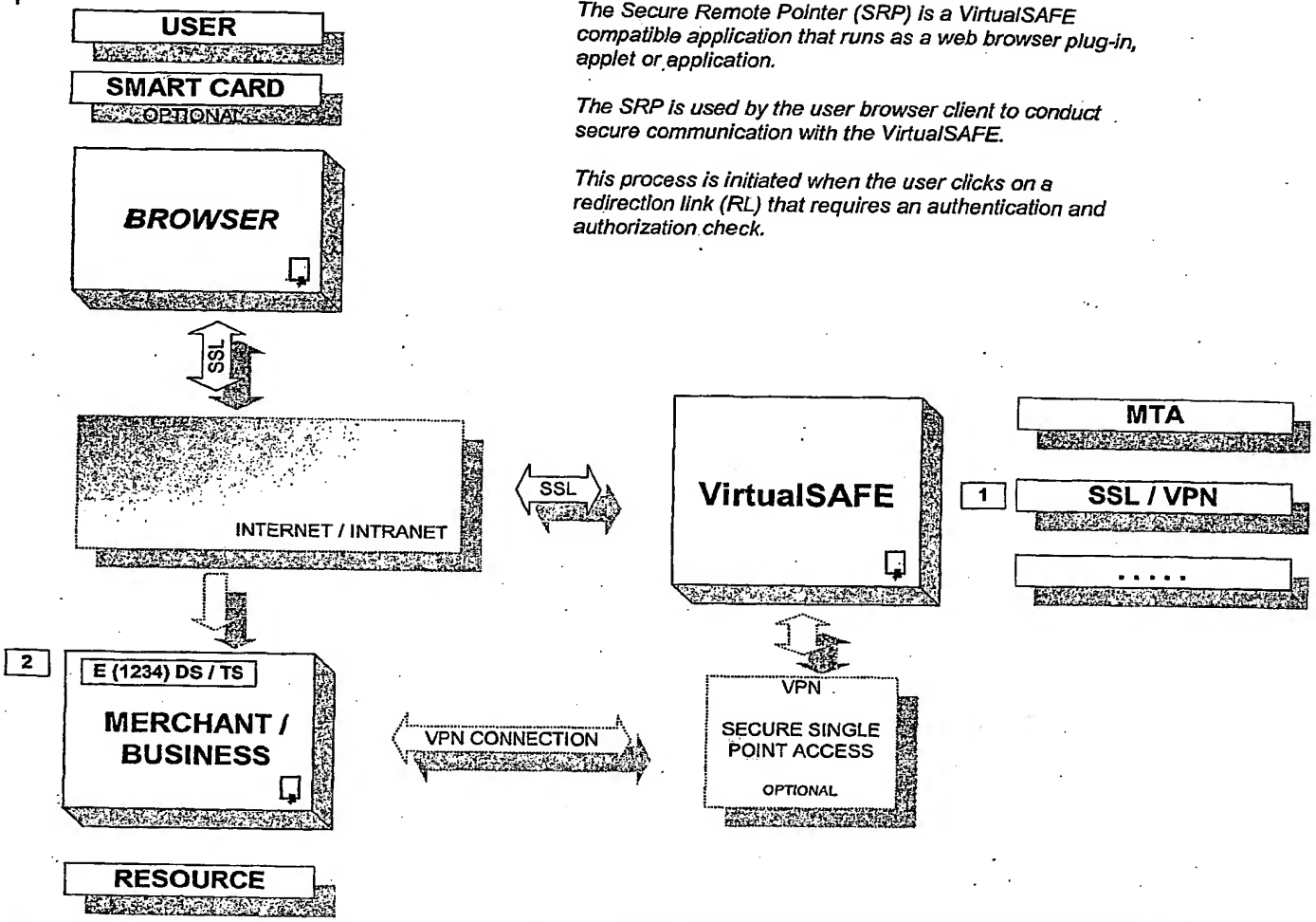
Online Transactions

1 - CUSTOMER BROWSES SITE
- BROWSER WITH CERTIFICATE
- SMART CARD APPLICATION WITH CERTIFICATE
- TOKEN WITH DIGITAL CERTIFICATE

2 - CUSTOMER/EMPLOYEE VirtualSAFE SECURED AND AUTHENTICATED ACCESS:
- CUSTOMER/EMPLOYEE/APPLICATION ACCESS CONTROL
- FULFILMENT
  - ONLINE BANKING
  - ONLINE BROKERAGE
  - MERCHANT
  - CREDIT/DEBIT CARD
  - ELECTRONIC CHECK
  - WIRE TRANSFER
  - ANY OTHER ONLINE APPLICATION OR SERVICE, ETC . . .
- VirtualSAFE Deposit Box (VSDB)
- OTHER VALUE SERVICES
  - SECURE E-MAIL
  - LOGISTIC SUPPORT FOR INDIVIDUAL, SMALL AND MEDIUM SIZE BUSINESSES
  - APPLICATION FRONT-END IS EASY TO UNDERSTAND AND USER FRIENDLY
  - APPLICATION IS ACCESSIBLE THROUGH INTERNET/INTRANET
  - VirtualSAFE IS INTEROPERABLE WITH EXISTING PROFESSIONAL OR CUSTOM APPLICATIONS
  - SECURE COLLABORATION PLACE

FIG. 15

Server Authentication



The Secure Remote Pointer (SRP) is a VirtualSAFE compatible application that runs as a web browser plug-in, applet or application.

The SRP is used by the user browser client to conduct secure communication with the VirtualSAFE.

This process is initiated when the user clicks on a redirection link (RL) that requires an authentication and authorization check.

SSL SERVER AUTHENTICATION

1 - VirtualSAFE SERVER INITIATES ONE-WAY SSL HANDSHAKE WITH USER

2 - SERVER AUTHENTICATION

- VirtualSAFE STORES TRANSMITTED INFORMATION
- VirtualSAFE QUERIES RECEIVED DIGITAL SIGNATURE

FIG. 16

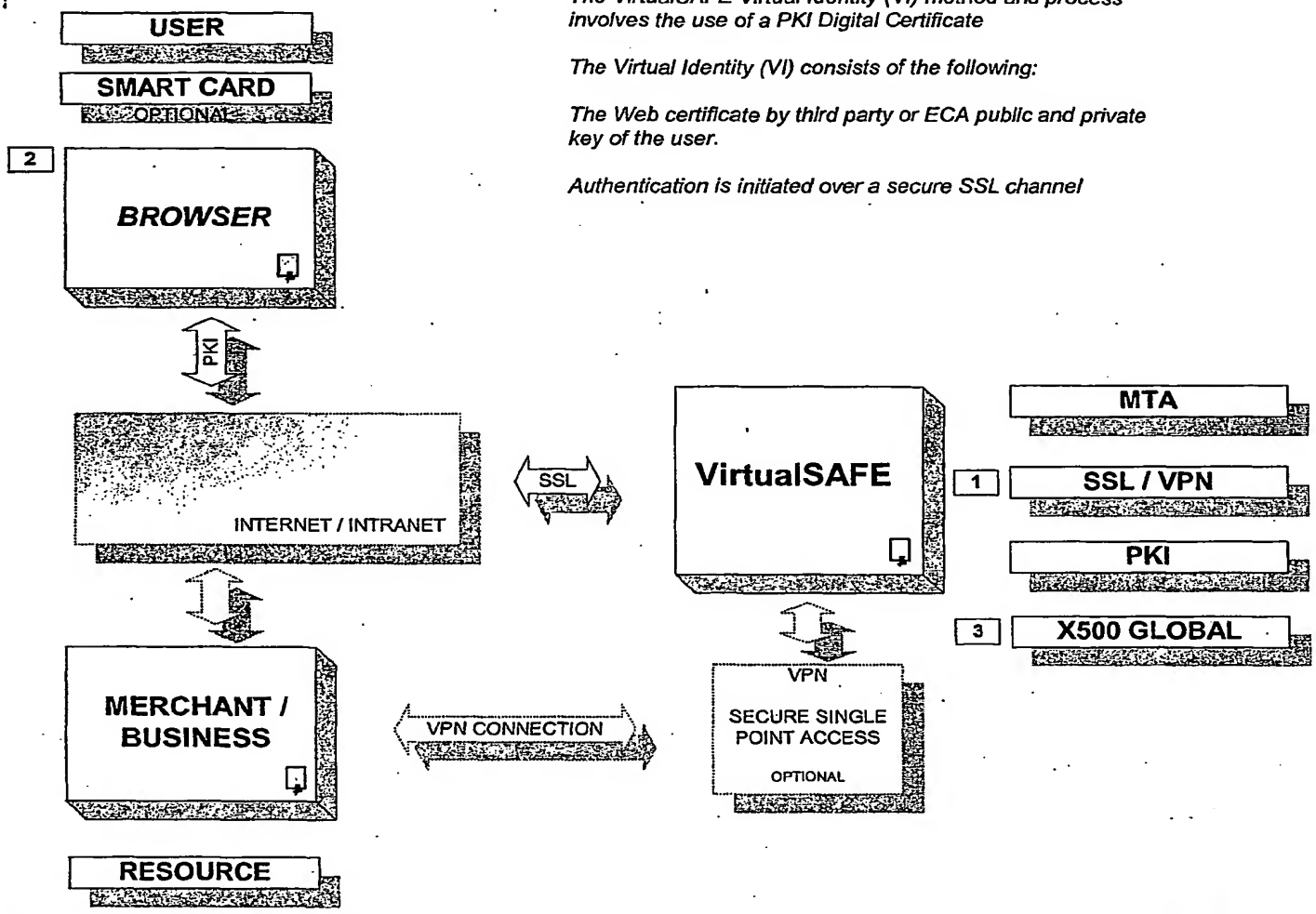
Computer Authentication

The VirtualSAFE Virtual Identity (VI) method and process involves the use of a PKI Digital Certificate

The Virtual Identity (VI) consists of the following:

The Web certificate by third party or ECA public and private key of the user.

Authentication is initiated over a secure SSL channel



AA - Authentication Authority

COMPUTER AUTHENTICATION

1 - VirtualSAFE SERVER INITIATES ONE-WAY SSL HANDSHAKE

2 - DIGITAL CERTIFICATE (PKI) ESTABLISHES TWO-WAY SSL HANDSHAKE

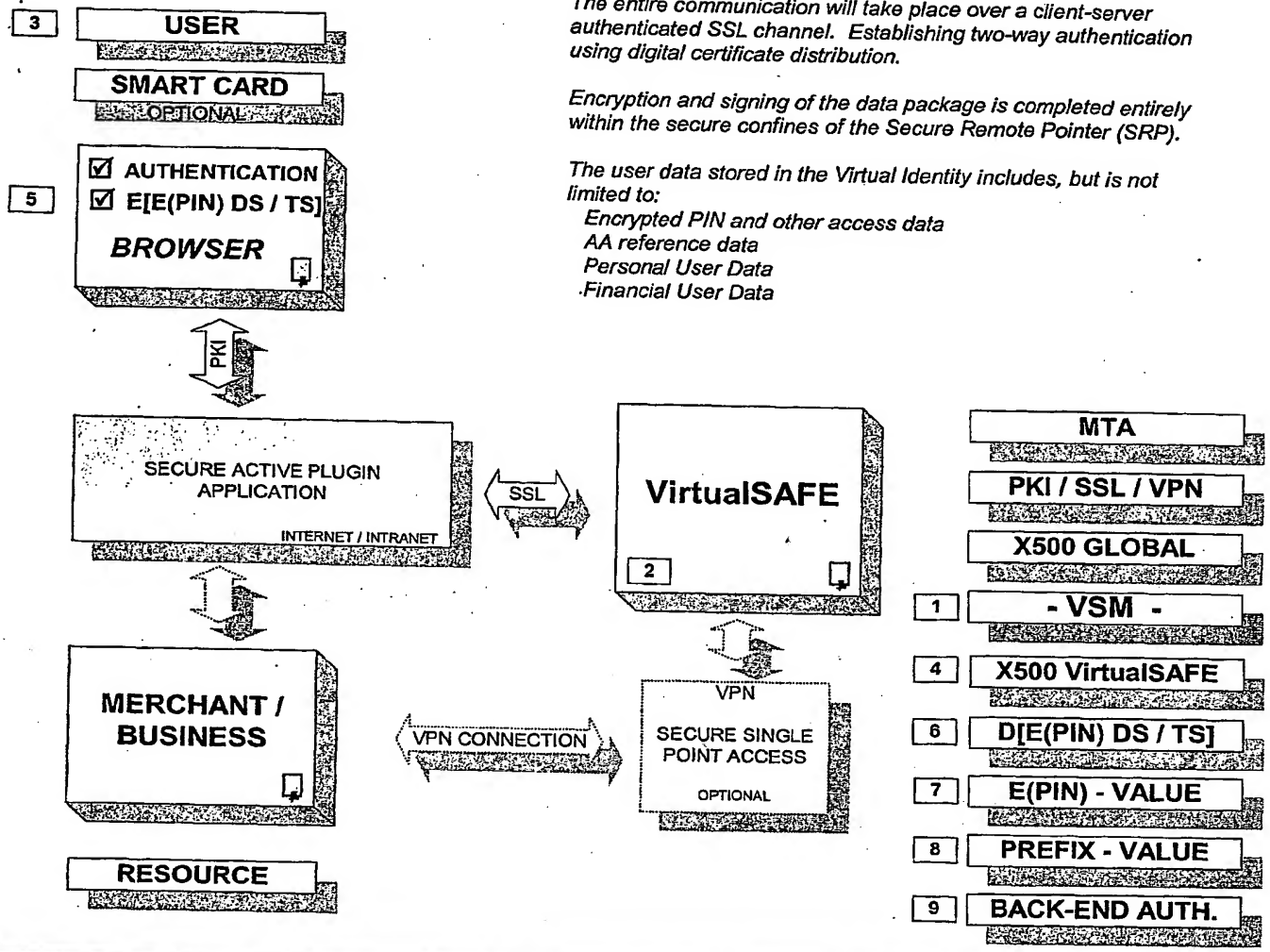
- VirtualSAFE INTEROPERABILITY FUNCTIONS
- VirtualSAFE IS X509 COMPATIBLE (ENTRUST, BALTIMORE, VERISIGN, ETC.)
- SECOND PHASE EC² (CERTICOM) COMPLIANT
- OTHER PKI STANDARD COMPLIANT (META, ETC.)

3 - VERIFICATION OF X500 GLOBAL DIRECTORY

- VirtualSAFE IS FULLY CAPABLE OF DETERMINING CERTIFICATE AUTHENTICITY BY VERIFYING PUBLIC DIRECTORIES (ENTRUST, BALTIMORE, VERISIGN, ETC.)

FIG. 17

User Authentication



The entire communication will take place over a client-server authenticated SSL channel. Establishing two-way authentication using digital certificate distribution.

Encryption and signing of the data package is completed entirely within the secure confines of the Secure Remote Pointer (SRP).

The user data stored in the Virtual Identity includes, but is not limited to:

- *Encrypted PIN and other access data*
- *AA reference data*
- *Personal User Data*
- *Financial User Data*

AA - Authentication Authority

USER AUTHENTICATION

1 - Virtual SMART CARD (VSC) ACTIVATED
- REMOTE VIRUS CHECK
- OPTIONAL KEY STROKE CHECK
- VirtualSAFE CERTIFICATE APPLICATION VALIDATION

2 - VirtualSAFE SECURE PLUG-IN / APPLICATION ACTIVATED

3 - USER PRESENTS IDENTIFICATION STRINGS

4 - Virtual SMART CARD IDENTIFIES USER IN VS X500 DIRECTORY

5 - USER'S PIN AND TIMESTAMP ARE TRIPLE ENCRYPTED - DIGITALLY SIGNED

6 - VirtualSAFE DECRYPTS DIGITALLY SIGNED USER'S PIN AND TIMESTAMP

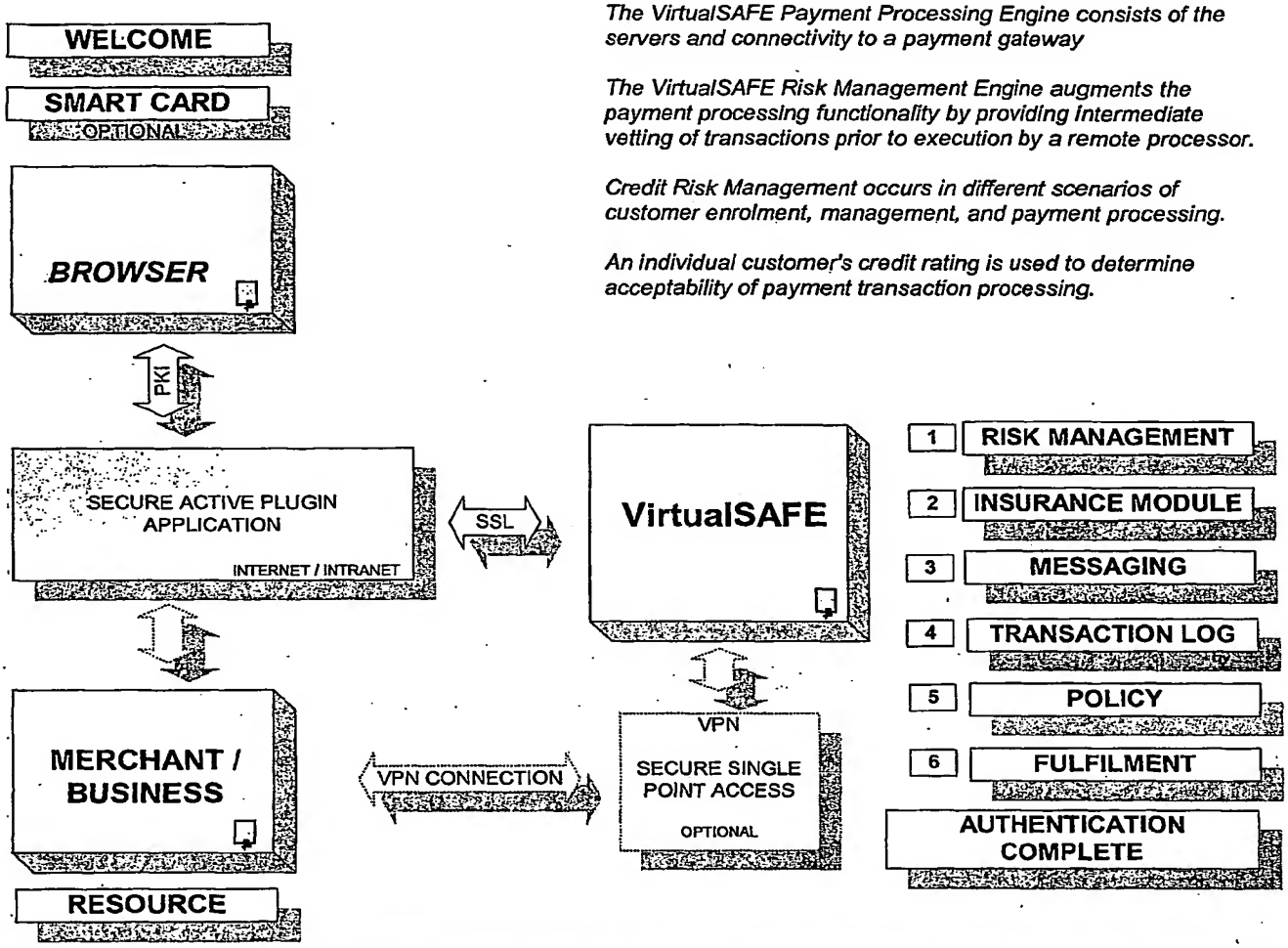
7 - USER ENCRYPTED PIN VALIDATED BY VirtualSAFE

8 - VirtualSAFE ENCRYPTED PREFIX VALIDATED BY SUPERVISOR

9 - VirtualSAFE PROCEEDS WITH BACK-END AUTHENTICATION

FIG. 18

Back-End Authentication



The VirtualSAFE Payment Processing Engine consists of the servers and connectivity to a payment gateway

The VirtualSAFE Risk Management Engine augments the payment processing functionality by providing intermediate vetting of transactions prior to execution by a remote processor.

Credit Risk Management occurs in different scenarios of customer enrolment, management, and payment processing.

An individual customer's credit rating is used to determine acceptability of payment transaction processing.

BACK-END AUTHENTICATION

1 - RISK MANAGEMENT
- INTERNAL SCORE VALUE VERIFICATION
- EXTERNAL SCORE VALUE VERIFICATION
- VirtualSAFE ASSESSMENT RESULT

2 - INSURANCE MODULE - POLICY ADJUSTABLE LIMIT
- BUSINESS LIABILITY - TRANSACTION VALUE
- USER LIABILITY POLICY - LIMITED BY CREDIT WORTH

3 - MESSAGING - E-MAIL OR NOTIFICATION
- INTERNAL - BUSINESS UNIT OR ADMINISTRATOR
- EXTERNAL - BUSINESS PARTNER OR USER

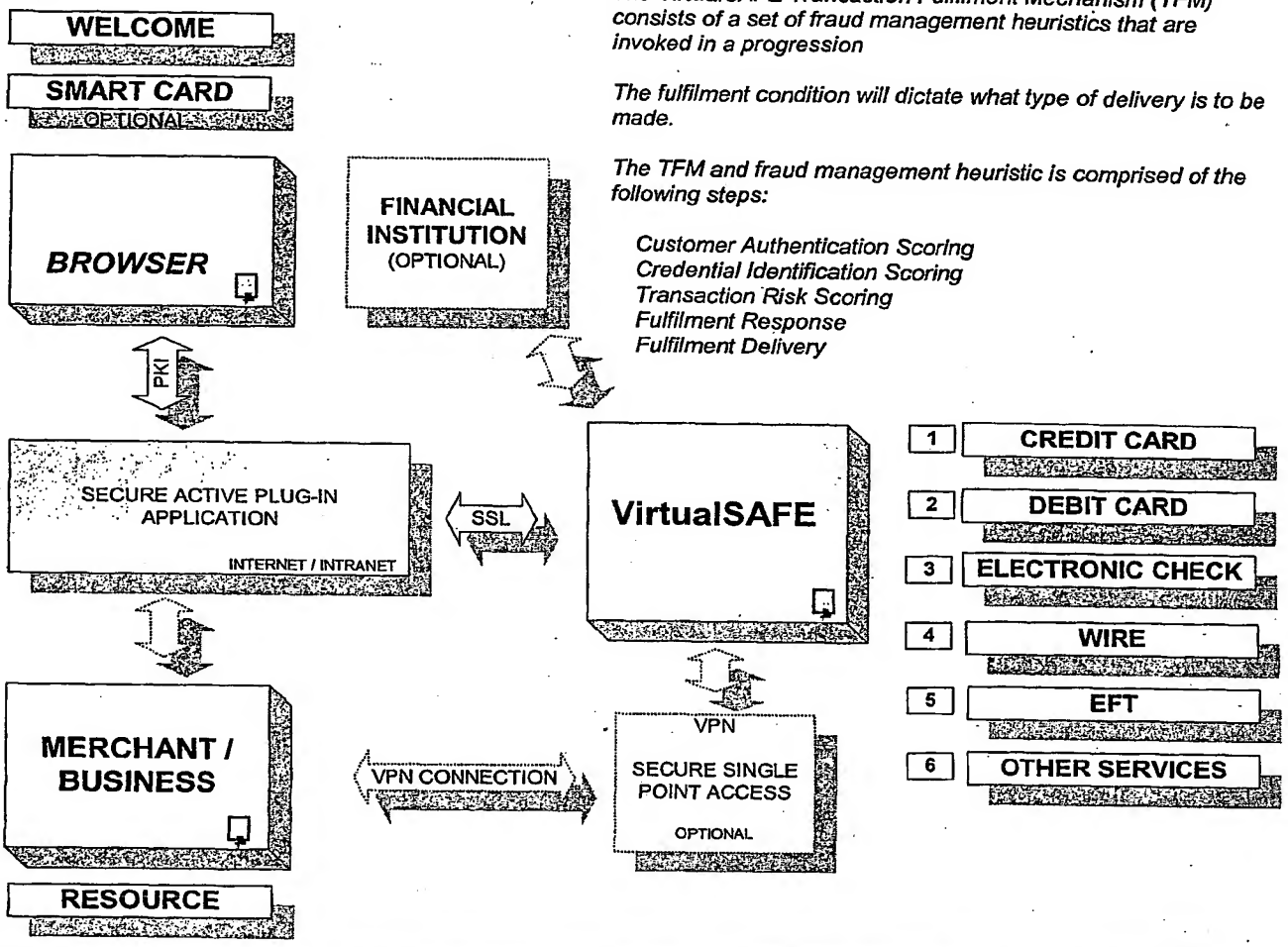
4 - VirtualSAFE ENCRYPTED TRANSACTION LOG

5 - POLICY
- PKI POLICY (PC AND PCA) REGULATED BY STANDARD PROCEDURE
- VirtualSAFE PRIVACY AND BUSINESS POLICY
- THIRD PARTY BUSINESS POLICY

6 - FULFILMENT PROCEDURE
- TRANSACTION
- COMMUNICATION
- DATA STORAGE
- ACCESS CONTROL
- ADMINISTRATION AND VirtualSAFE VALUE-ADDED SERVICES

FIG. 19

Fulfilment



The VirtualSAFE Transaction Fulfilment Mechanism (TFM) consists of a set of fraud management heuristics that are invoked in a progression

The fulfilment condition will dictate what type of delivery is to be made.

The TFM and fraud management heuristic is comprised of the following steps:

Customer Authentication Scoring
Credential Identification Scoring
Transaction Risk Scoring
Fulfilment Response
Fulfilment Delivery

AA - Authentication Authority

FULFILMENT

1 - ONLINE CREDIT CARD PAYMENT (SAME AS EFT)
2 - DEBIT CARD PAYMENT (SAME AS EFT)
3 - ELECTRONIC CHECK (SAME AS EFT)
4 - WIRE (SAME AS EFT)
5 - ELECTRONIC FUNDS TRANSFER (EFT), COIN PAYMENT, STORED-VALUE CARDS, ETC.
- SECURED TRANSACTIONS
- CUSTOMER AND MERCHANT AUDIT
- CUSTOMER AND MERCHANT LIABILITY INSURANCE
- TRANSACTION VALUE INSURANCE
- FRAUD CONTROL
- DELIVERY CONTROL
- LOYALTY PROGRAM

6 - OTHER SERVICES
- SECURE E-MAIL
- LOGISTIC SUPPORT FOR INDIVIDUAL, SMALL AND MEDIUM SIZE BUSINESSES
  - APPLICATION FRONT-END IS EASY TO UNDERSTAND AND USER FRIENDLY
  - APPLICATION IS ACCESSIBLE THROUGH INTERNET/INTRANET
  - VirtualSAFE IS INTEROPERABLE WITH EXISTING PROFESSIONAL OR CUSTOM APPLICATIONS
- SECURE COLLABORATION PLACE

FIG. 20

Attribute Authentication Authority

By definition access control entails the limiting of activities of a user on the system.

Enforcement of such controls is accomplished by maintaining a reference monitor that mediates access attempts by consulting an authorization base to determine if the user attempting the access is authorized to do so.

A distinction is made here between authentication and access control, where authentication merely confirms the identity of the user, while access control establishes identity privileges on the basis of successful authentication.

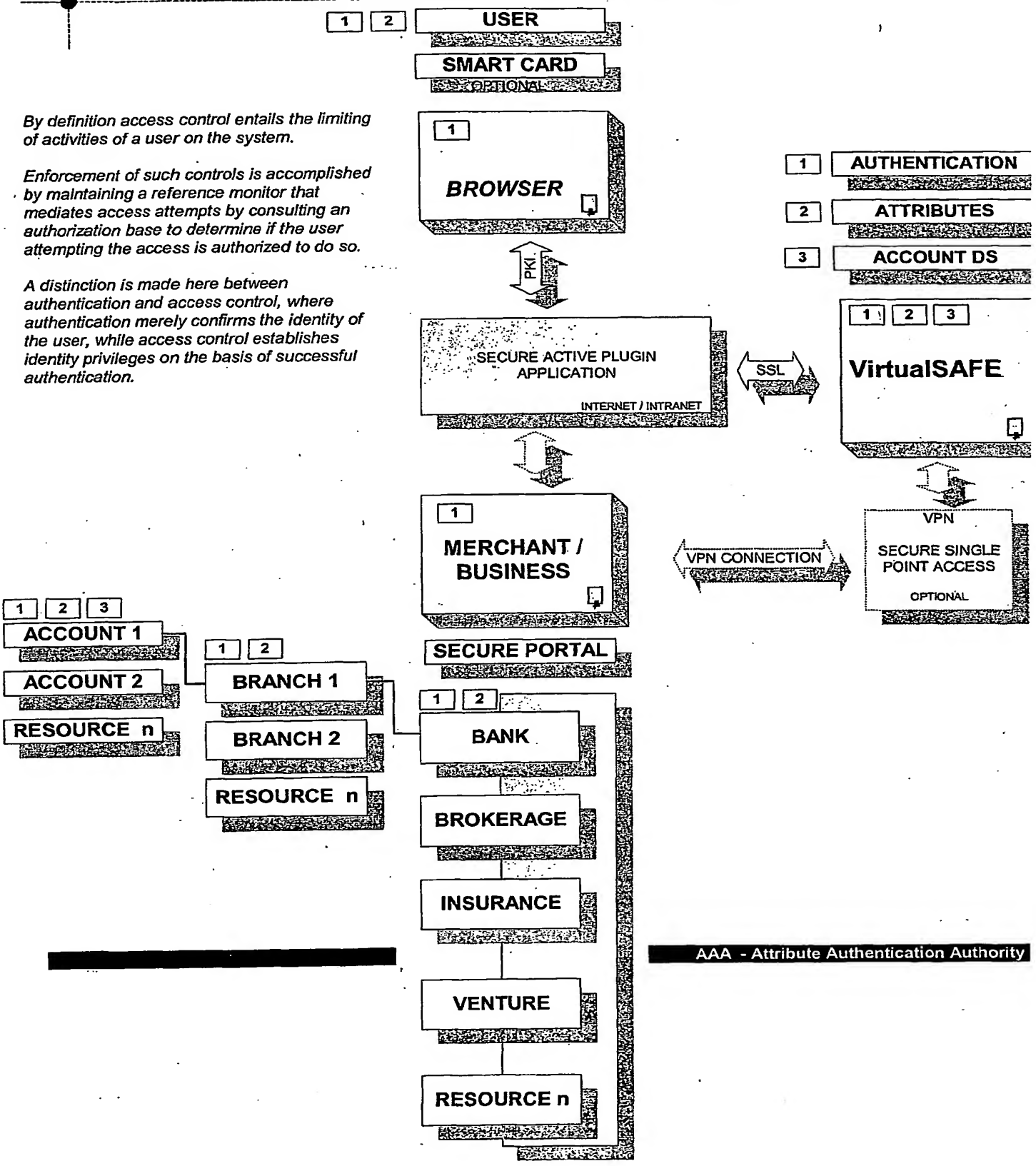
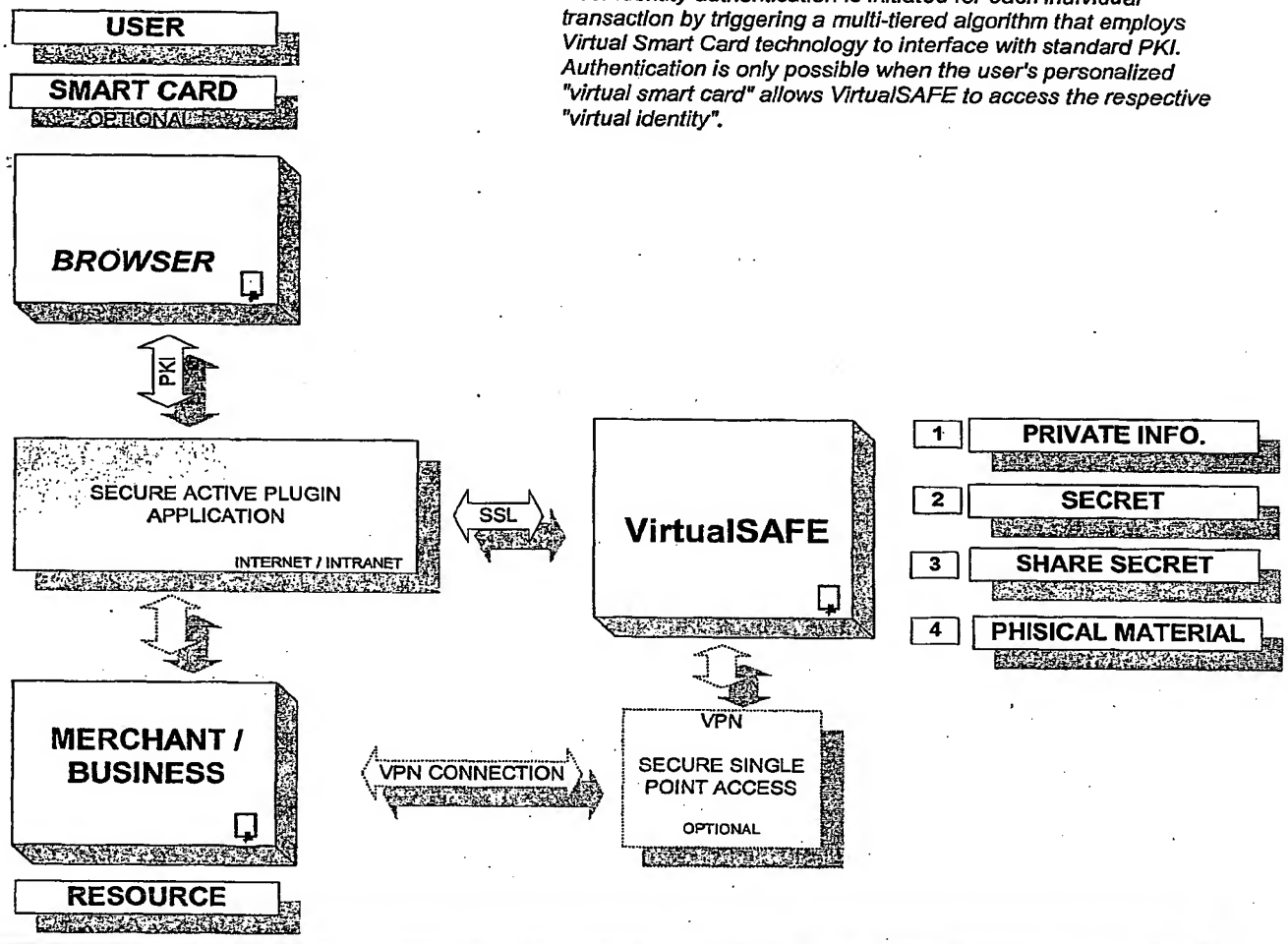


FIG. 21

Virtual Indentity (VI)



User identity authentication is initiated for each individual transaction by triggering a multi-tiered algorithm that employs Virtual Smart Card technology to interface with standard PKI. Authentication is only possible when the user's personalized "virtual smart card" allows VirtualSAFE to access the respective "virtual identity".

VIRTUAL INDENTITY (VI)

1 - VIRTUAL INDENTITY (VI) PRIVATE INFORMATION
- VI IS A PROPRIETARY ALGORITHM THAT IS USED TO CREATE AND MAINTAIN ENCRYPTED DATA FROM SOURCE DATA BASED ON PROVIDED AND VALIDATED INFORMATION

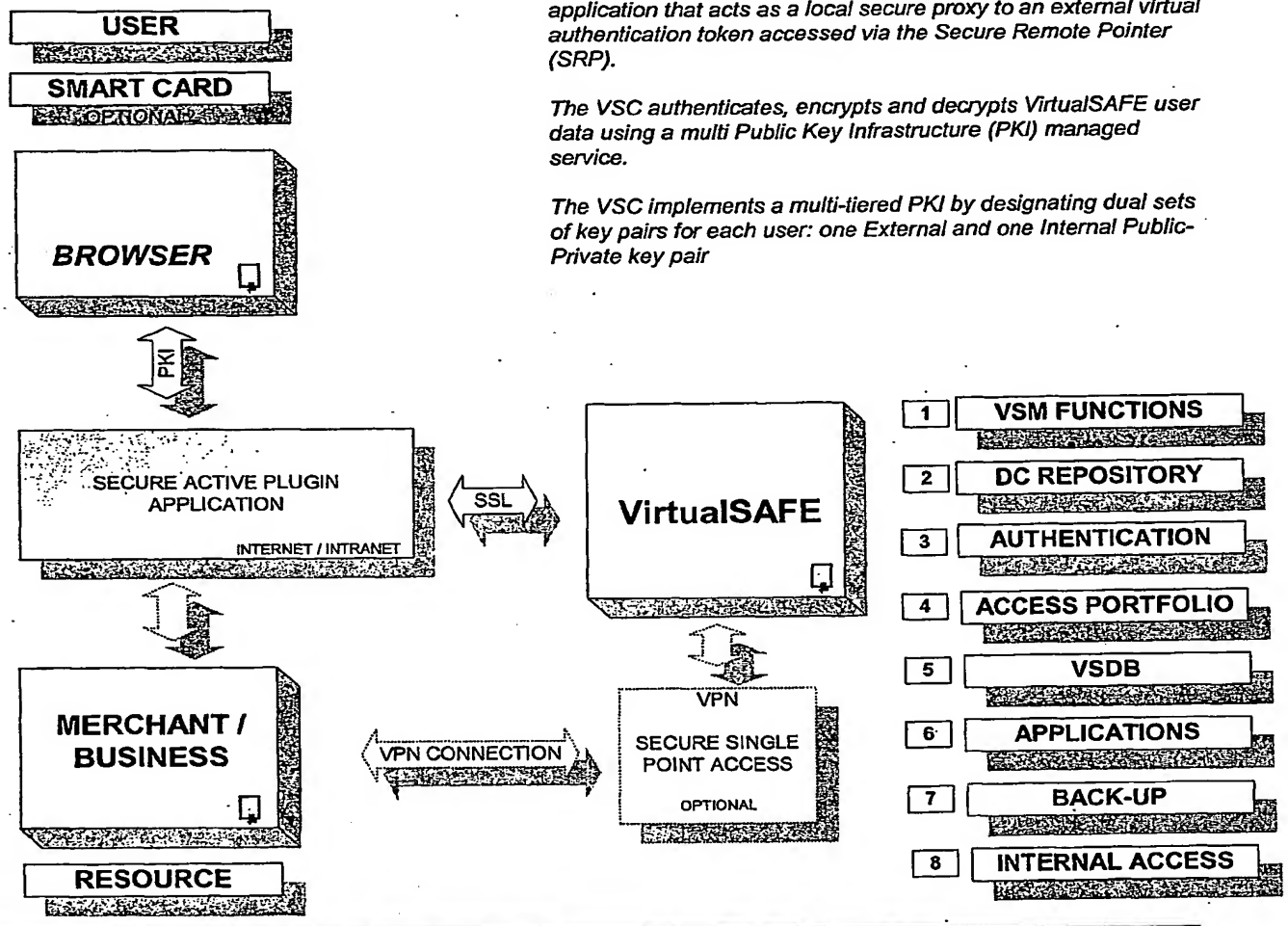
2 - VIRTUAL INDENTITY (VI) SECRET INFORMATION
- VI MAINTAINS THIS INFORMATION THAT IS ENCRYPTED AND ACCESSIBLE ONLY TO A SINGLE USER
- SECRET INFORMATION IS KNOWN ONLY BY THE USER WHOSE SECRET IT IS.

3 - VIRTUAL INDENTITY (VI) SHARE SECRET INFORMATION
- VI MAINTAINS THIS INFORMATION THAT IS ENCRYPTED AND ACCESSIBLE ONLY TO THE USER AND VirtuaSAFE PROXY
- SECRET INFORMATION IS KNOWN ONLY BY USER WHOSE SECRET IT IS AND BY THE VirtualSAFE PROXY

4 - VIRTUAL INDENTITY (VI) PHYSICAL MATERIAL
- PHYSICAL MATERIAL COULD BE REPRESENTED BY DIGITAL CERTIFICATE OR A UNIQUE SOFTWARE CODE (SCRIPT, PROGRAM OR SPECIAL CODE)
- PHYSICAL MATERIAL COULD BE:
  - LOCAL DIGITAL CERTIFICATE (PERSONAL COMPUTER, COMPUTER AND/OR WEB DIGITAL CERTIFICATE, SMART CARD, MAGNETIC CARD OR ANY DEVICE OPERATED BY THE USER)
  - VirtualSAFE CERTIFICATE (DIGITAL CERTIFICATE IS A DIGITAL CERTIFICATE STORED IN ANY TYPE OF REPOSITORY OR VirtualSAFE REPOSITORY MANAGED BY VirtualSAFE)
  - UNIQUE INDENTIFIER (IDENTIFIER ISSUED UNIQUELY TO A USER)
- TECHNOLOGICAL STANDARD
  - ENCRYPTION BASIS (RSA, CE² AND OTHER TYPES OF ALGORITHM)
  - PUBLIC KEY INFASTRUCTURE (PKI), X500, META, ETC.)

FIG. 22

Virtual Smart Card (VSC)



The Virtual Smart Card (VSC) is a VirtualSAFE internal application that acts as a local secure proxy to an external virtual authentication token accessed via the Secure Remote Pointer (SRP).

The VSC authenticates, encrypts and decrypts VirtualSAFE user data using a multi Public Key Infrastructure (PKI) managed service.

The VSC implements a multi-tiered PKI by designating dual sets of key pairs for each user: one External and one Internal Public-Private key pair

VIRTUAL SMART CARD (VSC)

1 - VIRTUAL SMART CARD (VSC) FUNCTIONS
- VSC IS THE EMULATION BASE OF THE READER AND SMART CARD ON REMOTE LOCATION
- VSC IS USED TO AUTHENTICATE USER ACCESS
- ALL INFORMATION BELONGING TO ENROLLED MEMBERS IS STORED AND PROTECTED BY A PROPRIETARY ENCRYPTION SCHEME USING A HIGH-SPEED HYBRID APPROACH
- VSC IS CO-ORDINATING PRIVACY POLICY

2 - VirtualSAFE DIGITAL CERTIFICATE (DC) REPOSITORY
- USERS REMOTE OR ROAMING DIGITAL CERTIFICATES STORED SECURELY

3 - AUTHENTICATION
- USER AUTHENTICATION USING VIRTUAL IDENTITY
- USER IDENTITY IS COMBINED WITH SECRETS, SHARED SECRETS AND PHYSICAL ELEMENTS (PKI)

4 - ACCESS PORTFOLIO
- PRIVATE, SHARED, BUSINESS OR GOVERNMENT

5 - VIRTUAL SAFE DEPOSIT BOX (VSDB)
- PERSONAL IDENTITY DATA (ID, DRIVERS LICENCE, ADDRESS, HEALTH CARD, ...)
- FINANCIAL INFORMATION (ACCOUNT NUMBERS, CREDIT/DEBIT CARD, WIRE, ...)
- BUSINESS (BUSINESS NUMBER AND ALL CONFIDENTIAL AND NON-CONFIDENTIAL DATA)
- GOVERMENT ((ID, DRIVERS LICENCE, ADDRESS, HEALTH CARD AND GOVERMENT CONFIDENTIAL AND NON-CONFIDENTIAL DATA)
- GENERAL REPOSITORY (DOCUMENTS AND ALL CONFIDENTIAL AND NON-CONFIDENTIAL DATA)
- TRANSACTION

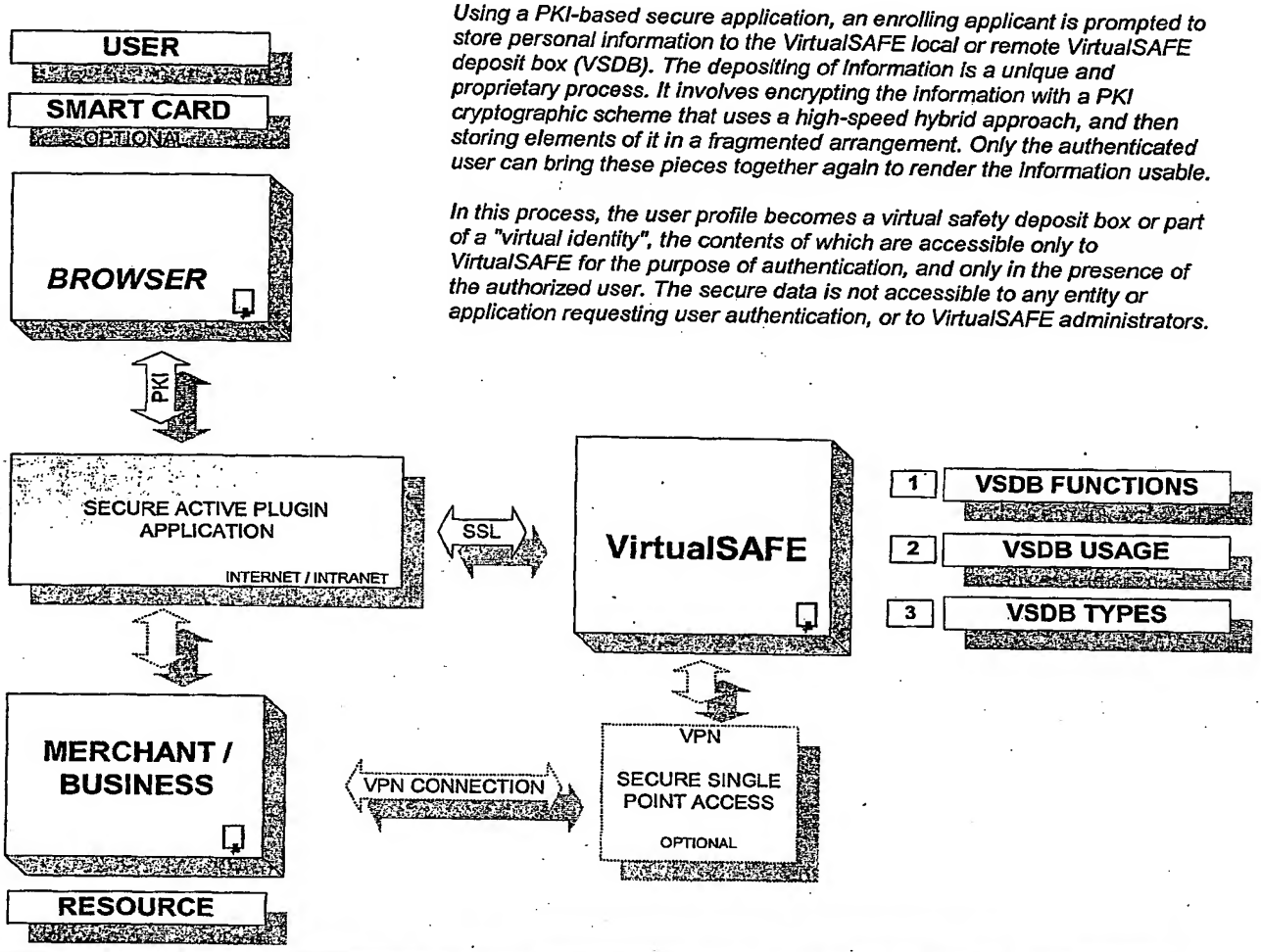
6 - APPLICATIONS
- REMOTE SOFTWARE LICENSING

7 - BACK-UP
- TRANSACTION LOGS
- TRANSACTION REVISIONS
- LOGS

8 - INTERNAL ACCESS
- VirtualSAFE, PRIVATE, SHARED, BUSINESS AND GOVERNMENT

FIG. 23

VirtualSAFE deposit box (VSDB)



Using a PKI-based secure application, an enrolling applicant is prompted to store personal information to the VirtualSAFE local or remote VirtualSAFE deposit box (VSDB). The depositing of information is a unique and proprietary process. It involves encrypting the information with a PKI cryptographic scheme that uses a high-speed hybrid approach, and then storing elements of it in a fragmented arrangement. Only the authenticated user can bring these pieces together again to render the information usable.

In this process, the user profile becomes a virtual safety deposit box or part of a "virtual identity", the contents of which are accessible only to VirtualSAFE for the purpose of authentication, and only in the presence of the authorized user. The secure data is not accessible to any entity or application requesting user authentication, or to VirtualSAFE administrators.

VirtualSAFE Deposit Box (VSDB)

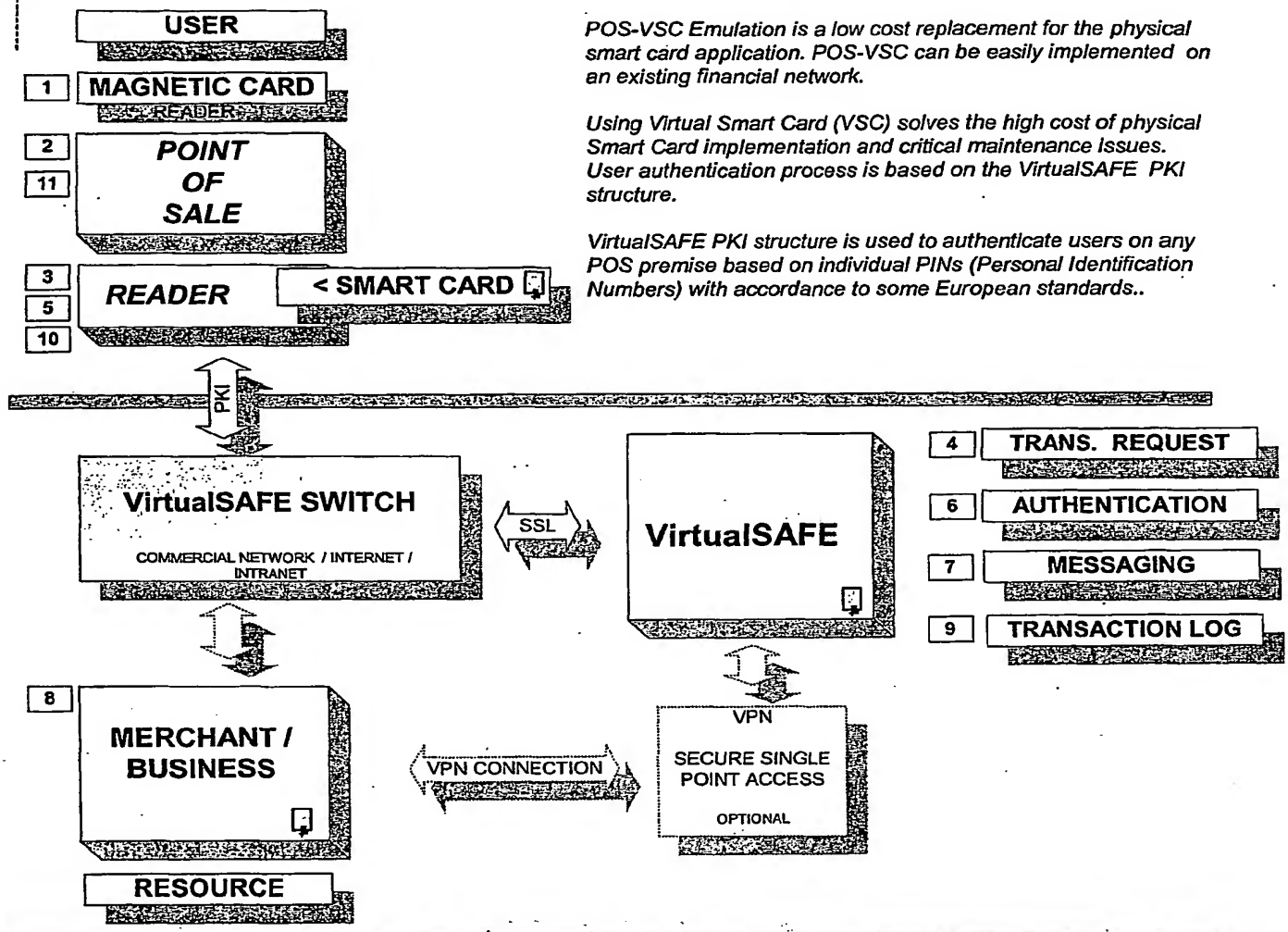
1 - VirtualSAFE Deposit Box (VSDB) FUNCTIONS
- VSDB IS A SECURED REMOTE STORAGE CONTROL WITH ACCESS CONTROL MAINTAINED BY THE VIRTUAL SMART CARD

2 - VirtualSAFE Deposit Box (VSDB) USAGE
- VSDB COULD BE OPERATED BY SINGLE OR MULTIPLE USERS
- USERS OF VSDB WILL HAVE DIFFERENT LEVELS OF PRIVILEGES BASED ON DEFINED POLICY
- USERS COULD COMMUNICATE AND STORE DATA IN THE FOLLOWING GENERAL FORMATS
  - MULTI-LINGUAL
  - MULTI-CALENDAR
  - MULTI-CURRENCY
  - MULTI-FORMAT (DOCUMENTS, DRAWINGS, FORMULAS AND ALL OTHER FILE FORMATS)

3 - VirtualSAFE Deposit Box (VSDB) TYPES
- VSDB SUPPORTS THE FOLLOWING DEPOSIT BOX FORMATS
  - PRIVATE (PRIVATE AND FAMILY RELATED INFORMATION AND THIRD PARTY AUTHENTICATION MECHANISMS - PIN's, ETC...)
  - FINANCIAL (ALL PRIVATE FINANCIAL RELATED AND BUSINESES/GOVERMENT FINANCIAL RELATED DATA)
  - BUSINESS (ALL BUSINESS RELATED DATA - BUSINESS NUMBERS, DOCUMENTS, LEGAL AND/OR HR DOCUMENTS, DRAWINGS, ETC..)
  - GOVERNMENT (ALL GOVERNMENT RELATED DATA - BUSINESS NUMBERS, DOCUMENTS, LEGAL AND/OR HR DOCUMENTS, DRAWINGS, ETC..)
  - GENERAL (COULD BE LOCAL OR REMOTE FOR CUSTOMER BASED ON POLICY)
  - TRANSACTION (COULD BE LOCAL AND REMOTE AND THIS TYPE OF VSDB SUPPORTS ALL DATA RELATED ALL TRANSACTIONS MAINTAINED BY VirtualSAFE - ALL PRIVATE INFORMATION IS ENCRYPTED AND MAINTAINED AS PER PRIVACY POLICY AND GOVERNMENT REGULATIONS)

FIG. 24

POS-VSC Emulation



POS-VSC Emulation is a low cost replacement for the physical smart card application. POS-VSC can be easily implemented on an existing financial network.

Using Virtual Smart Card (VSC) solves the high cost of physical Smart Card implementation and critical maintenance issues. User authentication process is based on the VirtualSAFE PKI structure.

VirtualSAFE PKI structure is used to authenticate users on any POS premise based on individual PINs (Personal Identification Numbers) with accordance to some European standards..

POINT OF SALE (POS) - VIRTUAL SMART CARD (VSC) EMULATION

1 - MAGNETIC CARD
- USER USES CREDIT/DEBIT MAGNETIC CARD

2 - POINT OF SALE (POS)
- POS REQUEST CREDIT/DEBIT CARD PAYMENT AUTHORIZATION

3 - SMART CARD READER
- MERCHANT SMART CARD IDENTIFIES MERCHANT/BUSINESS TO VirtualSAFE AND MERCHANT/BUSINESS
- RECEIVED MESSAGE FROM POS SENT TO VirtualSAFE

4 - TRANSACTION REQUEST
- VirtualSAFE RECEIVED TRANSACTION REQUEST
- VirtualSAFE REQUESTS USER PIN FOR AUTHENTICATION PURPOSES

5 - USER AUTHENTICATION PIN
- USER ENTERS PIN FOR AUTHENTICATION PURPOSES
- SMART CARD READER SENDS ENCRYPTED DATA TO VirtualSAFE

6 - AUTHENTICATION
- VirtualSAFE PROCESS AUTHENTICATES CUSTOMER

7 - MESSAGING
- PAYMENT REQUESTED FROM BANK

8 - PAYMENT PROCESSING
- CREDIT/DEBIT CARD PAYMENT AUTHORIZED / SETTLED

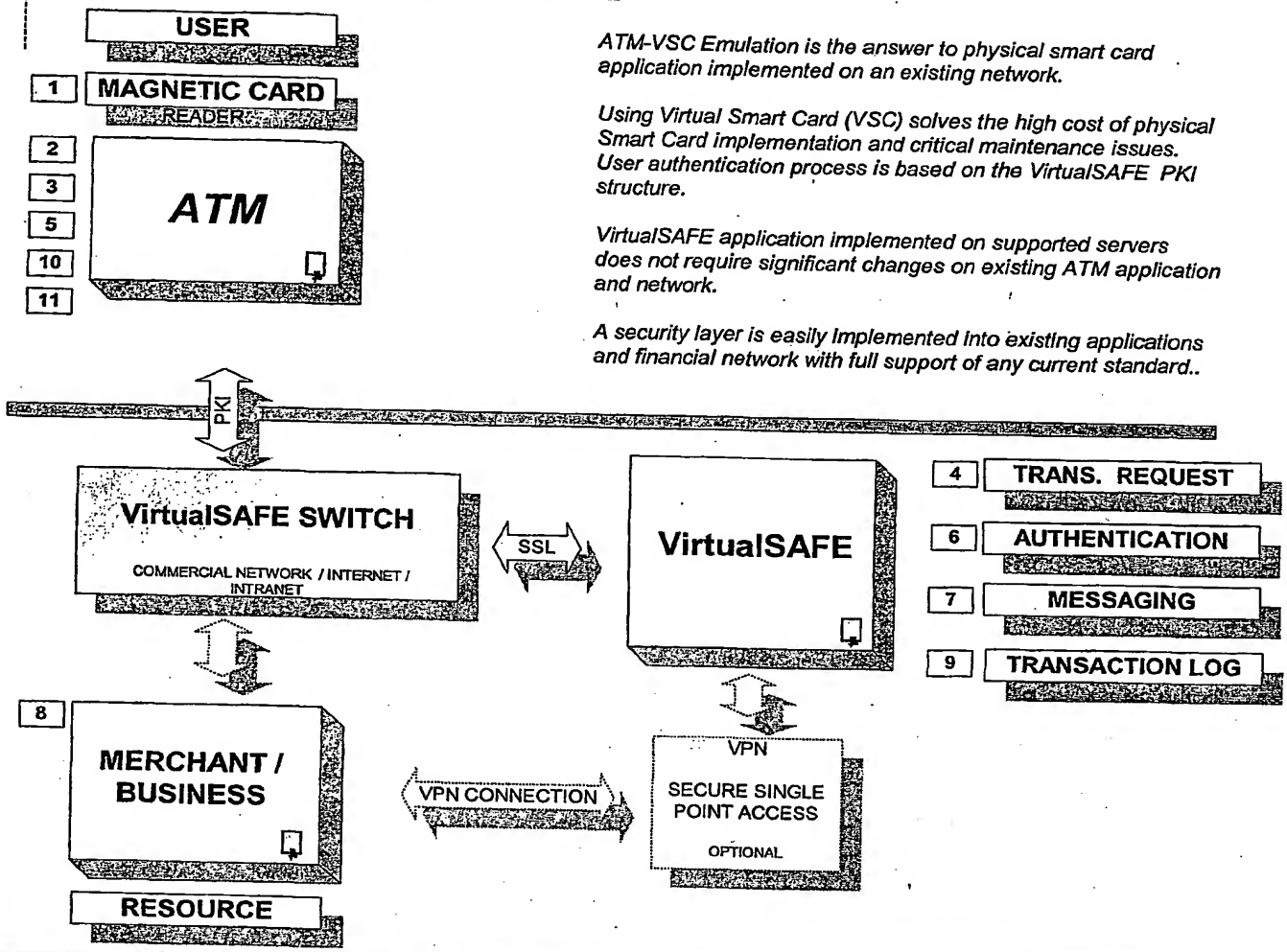
9 - TRANSACTION LOG
- MESSAGE SENT TO VirtualSAFE
- ALL TRANSACTION STEPS RECORDED

10 - SMART CARD READER CONFIRMATION
- SMART CARD READER RECEIVES AUTHORIZATION MESSAGE FROM CREDIT CARD PROCESSING DEPARTMENT
- DECRYPTED MESSAGE IS SENT TO POS

11 - POINT OF SALE AUTHORIZATION
- POS RECEIVES AUTHORIZED MESSAGE IN STANDARD FORMAT
- TRANSACTION AUTHORIZED AND PRINTED

FIG. 25

ATM-VSC Emulation



ATM-VSC Emulation is the answer to physical smart card application implemented on an existing network.

Using Virtual Smart Card (VSC) solves the high cost of physical Smart Card implementation and critical maintenance issues. User authentication process is based on the VirtualSAFE PKI structure.

VirtualSAFE application implemented on supported servers does not require significant changes on existing ATM application and network.

A security layer is easily Implemented into existing applications and financial network with full support of any current standard..

ATM - VIRTUAL SMART CARD (VSC) EMULATION

1 - MAGNETIC CARD
- USER USES CREDIT/DEBIT MAGNETIC CARD

2 - AUTOMATIC TELLER MACHINE (ATM)
- ATM REQUEST CREDIT/DEBIT CARD TRANSACTION AUTHORIZATION

3 - ADD-ON ATM APPLICATION
- ADD-ON ATM APPLICATION MAINTAINS DIGITAL CERTIFICATE WITH ALL SECURITY FUNCTIONS
- MAGNETIC READER READS CARD HASH INFORMATION
- DIGITAL CERTIFICATE ENCRYPTS AND SIGNS TRANSACTION AND PRIVATE INFORMATION

4 - TRANSACTION REQUEST
- VirtualSAFE RECEIVED TRANSACTION REQUEST
- VirtualSAFE REQUESTS USER PIN FOR AUTHENTICATION PURPOSES

5 - USER AUTHENTICATION PIN
- USER ENTERS PIN FOR AUTHENTICATION PURPOSES
- ATM SENDS ENCRYPTED DATA TO VirtualSAFE

6 - AUTHENTICATION
- VirtualSAFE PROCESS AUTHENTICATES CUSTOMER

7 - MESSAGING
- PAYMENT REQUESTED FROM BANK

8 - PAYMENT PROCESSING
- CREDIT/DEBIT CARD PAYMENT AUTHORIZED / SETTLED

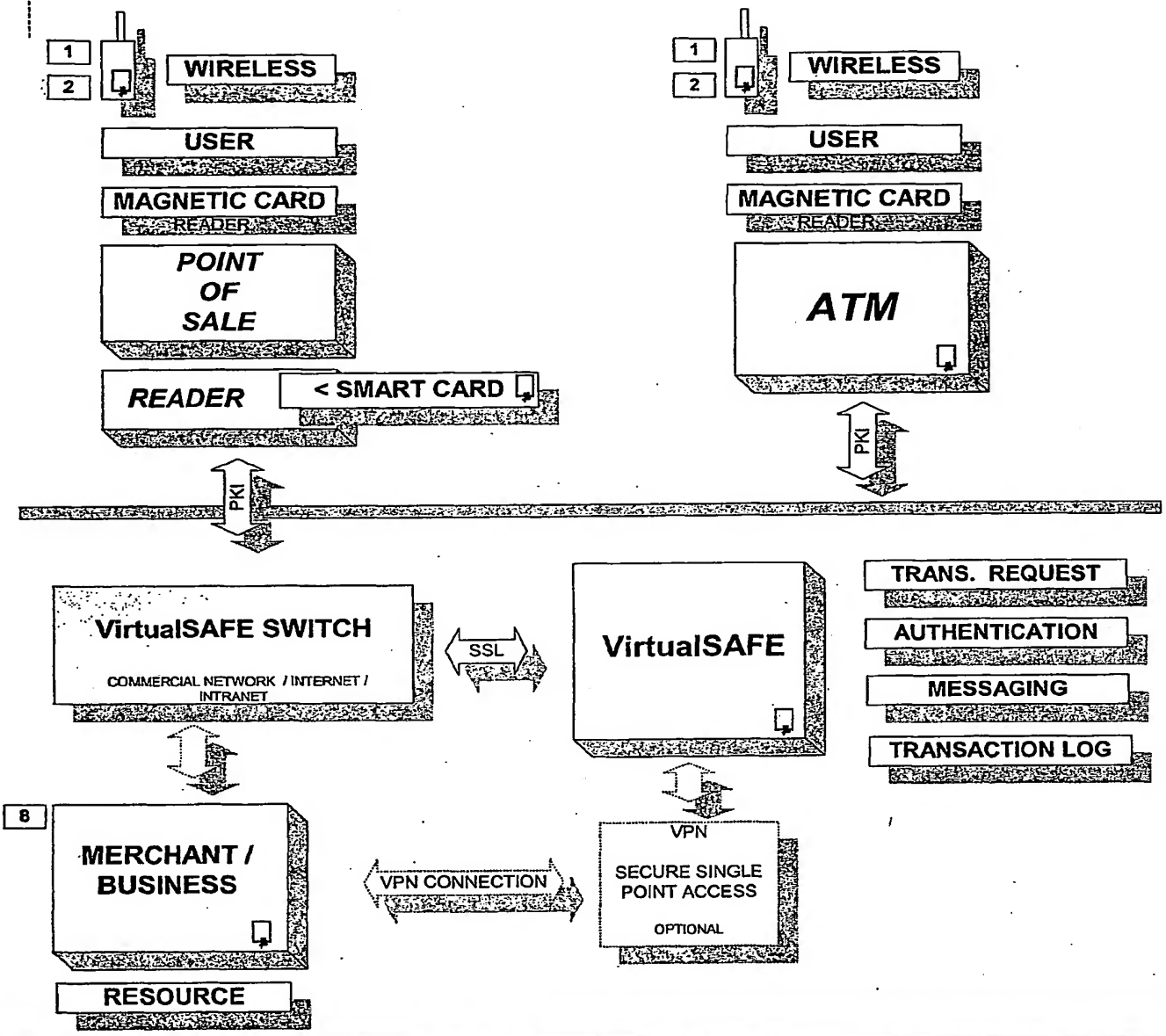
9 - TRANSACTION LOG
- MESSAGE SENT TO VirtualSAFE
- ALL TRANSACTION STEPS RECORDED

10 - ATM CONFIRMATION
- ATM RECEIVES AUTHORIZATION MESSAGE FROM CREDIT CARD PROCESSING DEPARTMENT

11 - ATM AUTHORIZATION
- TRANSACTION AUTHORIZED AND PRINTED

FIG. 26

POS / ATM/WIRELESS



AA - Authentication Authority

WIRELESS / POS / ATM VirtualSAFE APPLICATION

1 - WIRELESS VirtualSAFE ACCESS

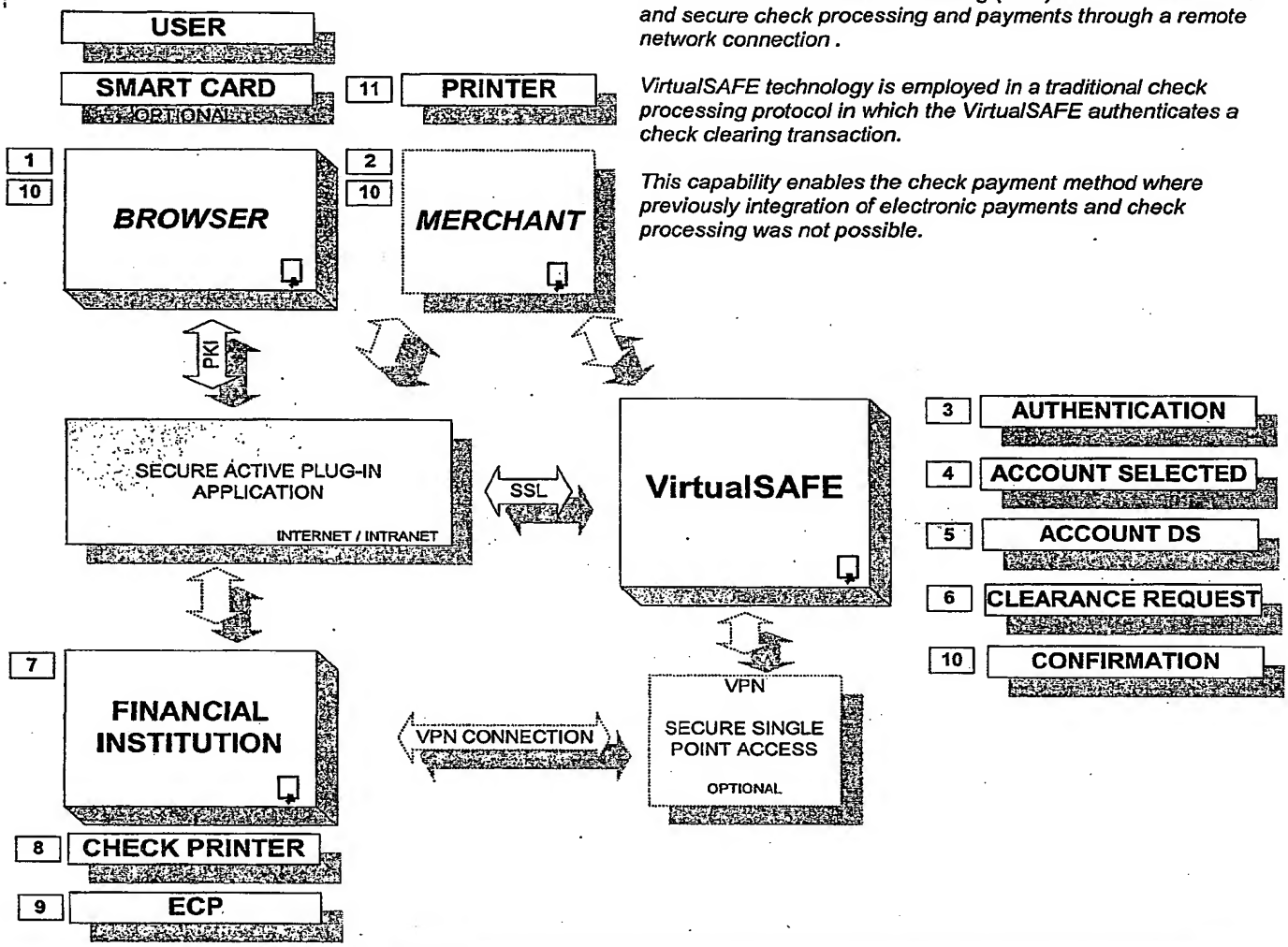
- USER ACCESSES VirtualSAFE THROUGH ANALOG OR DIGITAL WIRELESS NETWORK USING:
  - CELLULAR PHONES
  - PDA
  - TWO WAY RADIO
  - SATELLITE, ETC
- SECURE WIRELESS APPLICATION
  - LOCAL BASED
  - SERVER BASED
- TYPE OF COMMUNICATION
  - STANDARD WIRELESS NETWORK
  - LOCAL WIRELESS NETWORK
    - BLACKBERRY
    - BLUE TOOTH
    - INFRARED, ETC.

2 - LOCAL WIRELESS VirtualSAFE ACCESS

- USER ACCESSES LOCAL OR REMOTE VirtualSAFE WIRELESS APPLICATION.
  - LOCAL WIRELESS APPLICATION COMMUNICATES TO REMOTE DEVICE THROUGH CONVENTIONAL OR WIRELESS NETWORK
  - LOCAL WIRELESS AUTHENTICATION APPLICATION COMMUNICATES TO REMOTE VirtualSAFE DEVICE THROUGH CONVENTIONAL OR WIRELESS NETWORK

FIG. 27

SAFEcheck



The VirtualSAFE Check Processing (VCP) enables streamlined and secure check processing and payments through a remote network connection .

VirtualSAFE technology is employed in a traditional check processing protocol in which the VirtualSAFE authenticates a check clearing transaction.

This capability enables the check payment method where previously integration of electronic payments and check processing was not possible.

AA - Authentication Authority

SAFEcheck

1 - USER BROWSE MERCHANT SITE

2 - USER SELECTS SAFEcheck PAYMENT
- DIGITALLY SIGNED SHOPPING CART CONTENTS AND PAYMENT AMOUNTS SENT TO VirtualSAFE
- USER REDIRECTED TO VirtualSAFE SECURED SITE FOR FURTHER AUTHENTICATION

3 - USER AUTHENTICATION
- VirtualSAFE DEFINES AUTHENTICATION LEVEL DEPENDING ON PAYMENT AMOUNT AND SAFEcheck POLICY

4 - ACCOUNT SELECTED
- USER SELECTS APPROPRIATE CHECKING ACCOUNT FROM AVAILABILITY LIST

5 - ACCOUNT DIGITAL SIGNATURE (DS)
- USER DIGITALLY SIGNS SAFEcheck
- SAFEcheck SIGNED WITH WEB CERTIFICATE
- SAFEcheck SIGNED WITH VirtualSAFE CERTIFICATE

6 - CLEARANCE REQUEST
- VirtualSAFE ISSUES CLEARANCE REQUEST

7 - FINANCIAL INSTITUTION
- RECEIVES SAFEcheck FOR CHECK PRESENTMENT

8 - CHECK PRINTER
- SAFEcheck HAS BEEN PRINTED ON PREMISES INCLUDING CUSTOMER SIGNATURE
- PRINTER USES REGULATED CHECK PAPER WITH APPROPRIATE CODING

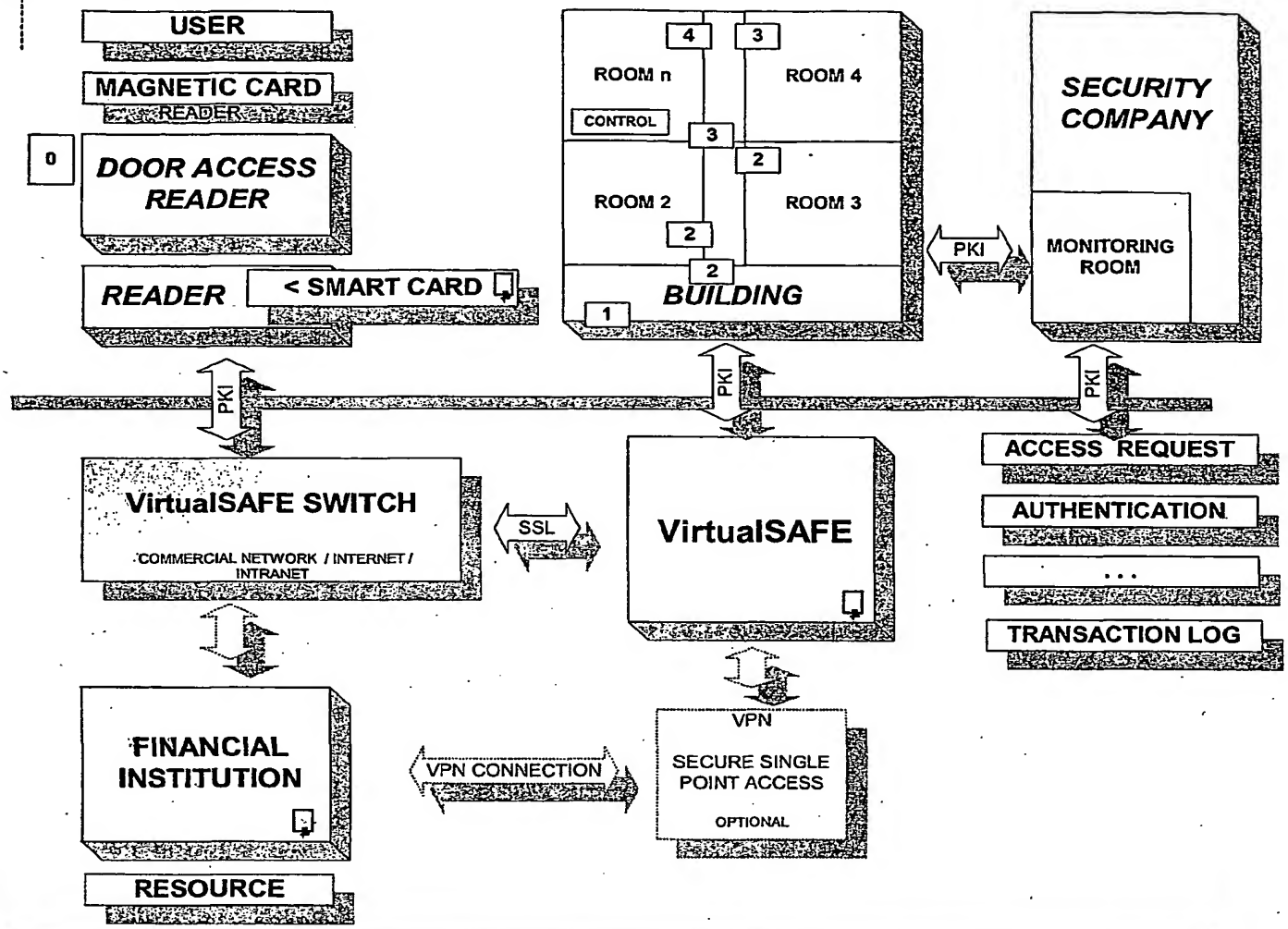
9 - ELECTRONIC CHECK PRESENTMENT (ECP)
- VirtualSAFE APPLICATION INTERFACES WITH ELECTRONIC CHECK PRESENTMENT MODULE
- SAFEcheck CLEARED AND PROCESSED

10 - CONFIRMATION
- VirtualSAFE RECEIVES CONFIRMATION
- VirtualSAFE SENDS CONFIRMATION TO MERCHANT AND USER TO COMPLETE TRANSACTION

11 - MERCHANT PRINTS SAFEcheck
- MERCHANT PRINTS OUT USER SIGNED COPY OF CLEARED CHECK
- USER OPTIONALLY SIGNS SAFEcheck AT MERCHANT PREMISES

FIG. 28

Physical Access Control



Physical Access Control

0 - EMPLOYEE/VISITOR DOOR ACCESS

- **LOCAL PHYSICAL ACCESS**
  - LOCAL OFFICE USER ACCESS REQUESTED
  - REQUEST IS PROCESSED LOCALLY
- **REMOTE PHYSICAL ACCESS**
  - REMOTE OFFICE USER ACCESS REQUESTED
  - REQUEST IS PROCESSED REMOTELY
- **VirtualSAFE CONTROLLED HIGH SECURITY ACCESS**
  - REMOTE OFFICE USER ACCESS REQUESTED
  - REQUEST IS PROCESSED REMOTELY

1 - ENTRY LEVEL 1

- BUILDING USER REQUESTS ACCESS TO LOCAL BRANCH
- BUILDING CONTROL UNIT VALIDATES DIGITAL CERTIFICATE ACCESS LEVEL AND AUTHORIZES ACCESS

2 - ENTRY LEVEL 2

- BUILDING USER REQUESTS ACCESS TO BUILDING **SECURED** ROOM
- BUILDING CONTROL UNIT VALIDATES DIGITAL CERTIFICATE ACCESS LEVEL AND REQUESTS USER PIN

3 - ENTRY LEVEL 3

- BUILDING USER REQUESTS ACCESS TO BUILDING **HIGH SECURED** ROOM
- BUILDING CONTROL FORWARDS VALIDATION OF THE DIGITAL CERTIFICATE FROM SECURITY COMPANY CONTROLLER
- USER MUST PROVIDE PIN

4 - ENTRY LEVEL 4

- BUILDING USER REQUESTS ACCESS TO BUILDING **RESTRICTED AREA**
- BUILDING CONTROL FORWARDS VALIDATION OF THE DIGITAL CERTIFICATE FROM VirtualSAFE THROUGH SECURITY COMPANY
- USER MUST PROVIDE VirtualSAFE PIN

FIG. 29

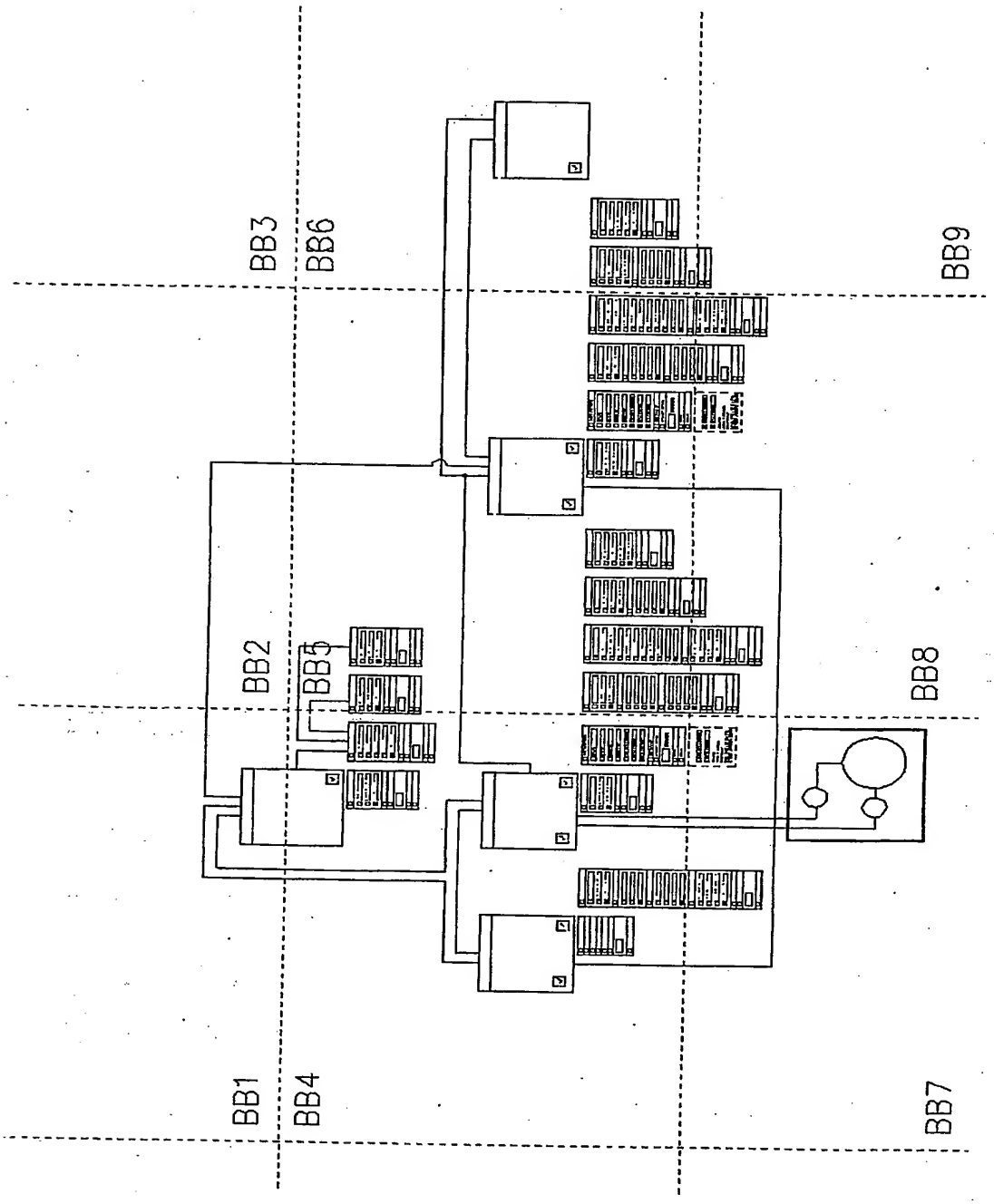


FIG. 30

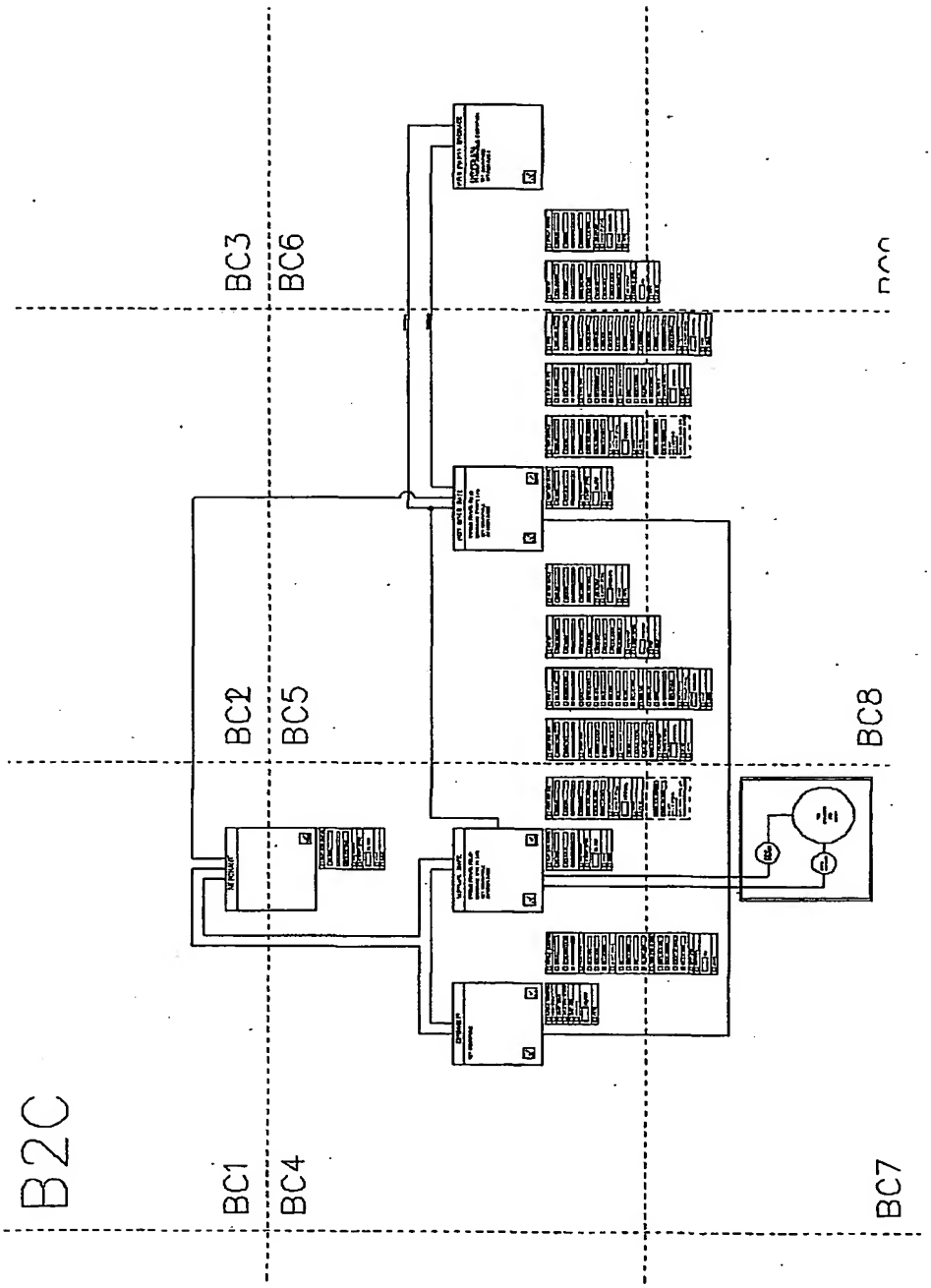


FIG. 31

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 01/00504

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) figures 1-3 column 3, line 33 -column 5, line 24 column 6, line 12 -column 8, line 14	1-3
X	EP 0 982 692 A (IBM) 1 March 2000 (2000-03-01) figure 2 paragraph '0012! - paragraph '0020!	1-3
X	EP 0 936 530 A (SIEMENS NIXDORF INF SYST) 18 August 1999 (1999-08-18) figures 1,2 paragraph '0011! - paragraph '0017! paragraph '0019! - paragraph '0028! paragraph '0034! - paragraph '0041!	1-3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 September 2001	20/09/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	**Authorized officer** Papastefanou, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 01/00504

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 814 441 A (FRANCE TELECOM) 29 December 1997 (1997-12-29) page 4, line 56 -page 6, line 43	1-3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTER[redacted]ONAL SEARCH REPORT

[redacted]ial Application No
PCT/CA 01/00504

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5883810 A	16-03-1999	NONE	
EP 0982692 A	01-03-2000	DE 19838628 A1	02-03-2000
		EP 0982692 A2	01-03-2000
		JP 2000194660 A	14-07-2000
EP 0936530 A	18-08-1999	EP 0936530 A1	18-08-1999
EP 0814441 A	29-12-1997	FR 2750274 A1	26-12-1997
		EP 0814441 A1	29-12-1997
		JP 10079006 A	24-03-1998
		US 5991413 A	23-11-1999